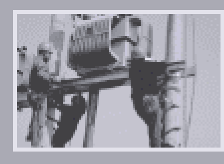
电力终端通信接入网
规划与运维技术

沈　力　主编







清华大学出版社

电力终端通信接入网规划与运维技术

沈　力　主编

清華大学出版社
北　京

内 容 简 介

本书以终端通信接入网的基本架构为主线，以电力业务应用为场景，以网络资源、接入技术为基础，以业务需求为导向，旨在对电力终端通信接入网进行全面梳理，为形成具有适用性强、灵活性高、易操作的终端通信接入网规划与运维技术提供理论支撑。

全书共8章，第1～4章为基础资源分布和技术条件、业务应用场景与应用需求分析、业务与接入网技术匹配性分析、规划和运维技术需求分析，均以业务应用为出发点，是电力终端通信接入网的分析基础；第5～7章为电力终端通信接入网规划、典型组网模式、电力终端通信接入网运维技术，均以业务与技术的应用为结合点，对电力终端通信接入网的规划和运维技术进行了讨论和研究，第8章梳理了电力终端通信接入网新技术，并结合电力应用场景进行展望。

本书对全国电力终端通信网以及通信接入网的建设有重要参考价值和现实指导意义，可供从事电力系统通信研究和规划建设的科技人员参考，也可供对终端通信接入技术在电力场景中应用感兴趣的读者阅读。

图书在版编目(CIP)数据

电力终端通信接入网规划与运维技术 / 沈力主编. — 北京：清华大学出版社，2018
ISBN 978-7-302-50131-2

Ⅰ. ①电… Ⅱ. ①沈… Ⅲ. ①电力通信系统—研究 Ⅳ. ①TN915.853

中国版本图书馆 CIP 数据核字（2018）第 093817 号

责任编辑：杨如林
封面设计：杨玉兰
责任校对：李建庄
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：21.75　　字　　数：471 千字
版　　次：2018 年 7 月第 1 版　　印　　次：2018 年 7 月第 1 次印刷
印　　数：1 ～ 2000
定　　价：69.00 元

产品编号：079259-01

编委会名单

前　言

终端通信接入网是电力通信网的重要组成部分,是电力骨干通信网的延伸，是配、用电终端与主站信息交互的核心平台。随着智能电网建设的开展，面对配电网的发展与营配调贯通等新形势和新需求以及新兴业务的展开，如何构建“架构合理、性能可靠、安全可控、成本适中”的接入网，应用技术手段实现从规划到运维的全环节专业化管理，始终是公司各业务部门、研发以及产业支撑单位需要攻克的重大命题。建设多手段、多功能、全业务、全覆盖的终端通信接入网，能有效提升配用电网的安全生产和对外的优质服务，对落实公司全球能源互联网发展的战略意义重大。

本书针对终端通信接入网承载业务的特征，结合现有终端通信接入网的基础资源、技术要求、业务需求、存在问题、规划与运维需求与目标，辅以作者多年来在终端通信接入网技术及管理领域的研究成果和参与国家相关重大项目的经验，系统地分析了电力终端通信接入网规划与运维工作的基础理论。本书第1章介绍了电力终端通信接入网的业务资源、网络资源、存在的问题和现有的技术条件；第2章介绍了业务应用场景模型和应用需求，并进行多业务公共接入分析；第3章介绍了终端通信接入网的技术体系，并进行了技术匹配性分析；第4章分析了终端通信接入网规划及运维需求，并进行运维评价体系研究；第5章主要对终端通信接入网的业务接入需求、传输速率、系统容量、延时、安全稳定性要求进行分析，提出业务控制技术、等级映射技术、网络优化技术等一系列适用于终端通信接入网的规划手段；第6章根据业务需求梳理了终端通信接入网承载的所有业务典型的接入场景以及技术特征，并进行了经济性分析；第7章介绍了运行监视与故障分析技术、性能分析与探测技术，并提出故障检测与定位的方法，给出了电力的典型应用环境，同时从部署策略、管理策略等方面进行了探索；第8章对有线专网、PON、宽带电力线载波、北斗、宽带卫星通信、可信计算、量子通信、光锁、区块链等新兴技术进行了研究，并对新技术在电力场景的应用路线进行预测。

本书由国家电网公司、国网辽宁省电力有限公司、国网信息通信产业集团有限公司、国网冀北电力有限公司、国网内蒙古东部电力有限公司、华北电力大学、中国信息通信研

究院、东北大学、辽宁邮电规划设计院有限公司等单位相关专家策划并编写。衷心感谢清华大学出版社对本书出版工作的大力支持！

由于作者水平有限，编写时间较为仓促，书中内容难免会出现疏漏与不当之处，敬请读者批评指正。

作　者

2018年5月

目　　录

第1章

基础资源分布和技术条件



1.1 业务资源分布情况

1.1.1 终端通信接入网的概念

终端通信接入网按照配用电环节的发展需要建设，它分为有线和无线两种组网模式，主要满足配电自动化、用电信息采集、分布式电源接入、电动汽车充电站（桩）等通信业务的接入和上联需求，形成与骨干传输网垂直贯通、面向用户、安全可控的一体化接入网络。

接入网由业务站点接口和用户网络接口之间一系列传送实体（如线路设施和传输设施等）组成，提供配电与用电业务站点同电力骨干通信网络的连接，实现配用电业务站点与系统间的信息交互，具有业务承载和信息传送功能。

接入网分为10kV接入网和0.4kV接入网两部分。10kV接入网主要覆盖10kV配电网开关站、配电室、环网单元、柱上开关、配电变压器、分布式能源站点、电动汽车充换电站、10kV配电线路等。0.4kV接入网主要覆盖10kV配电变压器至用户电表、电动汽车充电桩、分布式能源站点等，并延伸至用户室内，用于实现双向互动用电服务、智能家电控制及增值业务服务，主要承载用户用电信息采集本地通道、电力光纤到户等业务。

1.1.2 配电自动化

配电自动化系统以一次网架和设备为基础，综合利用计算机、信息及通信等技术，并通过与相关应用系统的信息集成，实现对配电网的监测、控制和快速故障隔离。配电自动化系统是实现配电网运行监视和控制的自动化系统，具备配电SCADA（Supervisory Control And Data Acquisition）、馈线自动化、故障处理、分析应用及与相关应用系统互连等功能。

目前，配电自动化业务所采用的通信方式有EPON、工业以太网交换机、无线专网、中压电力线载波和无线公网。各种通信组网方式架构如图1-1所示。

按照配电自动化站点是否需要实现三遥（遥信、遥测、遥控）功能来划分，三遥站点采用EPON或工业以太网交换机的通信方式；对于不需要遥控功能的站点，采用以光纤专网通信为主，中压电力线载波及无线专网通信为辅的通信方式，在光缆敷设较为困难的区

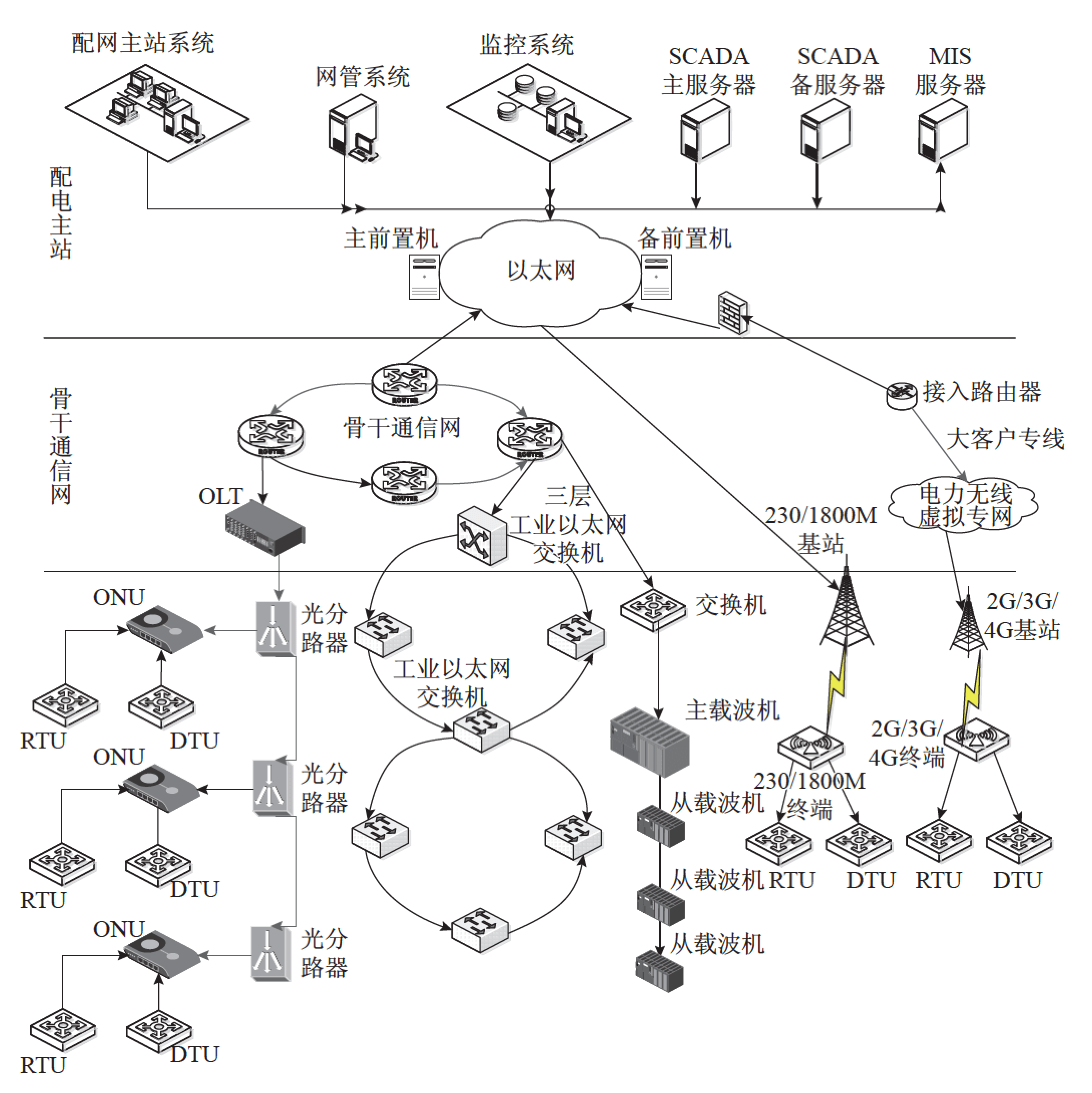


图1-1 配电自动化业务通信组网示意图

域，可采用无线公网的通信方式。采用无线公网通信时，需通过无线虚拟专网，经过大客户专线进入部署于地市调控中心的配电自动化主站。

1.1.3 用电信息采集

用电信息采集系统是对电力用户的用电信息进行采集、处理和实时监控的系统，实现用电信息的自动采集、计量异常监测、电能质量监测、用电分析和管理、相关信息发布、分布式能源监控、智能用电设备的信息交互等功能，由采集主站、通信通道和采集终端组成。

用电信息采集的远程通信方式有EPON、无线专网和无线公网等。各种通信方式的组网架构如图1-2所示。

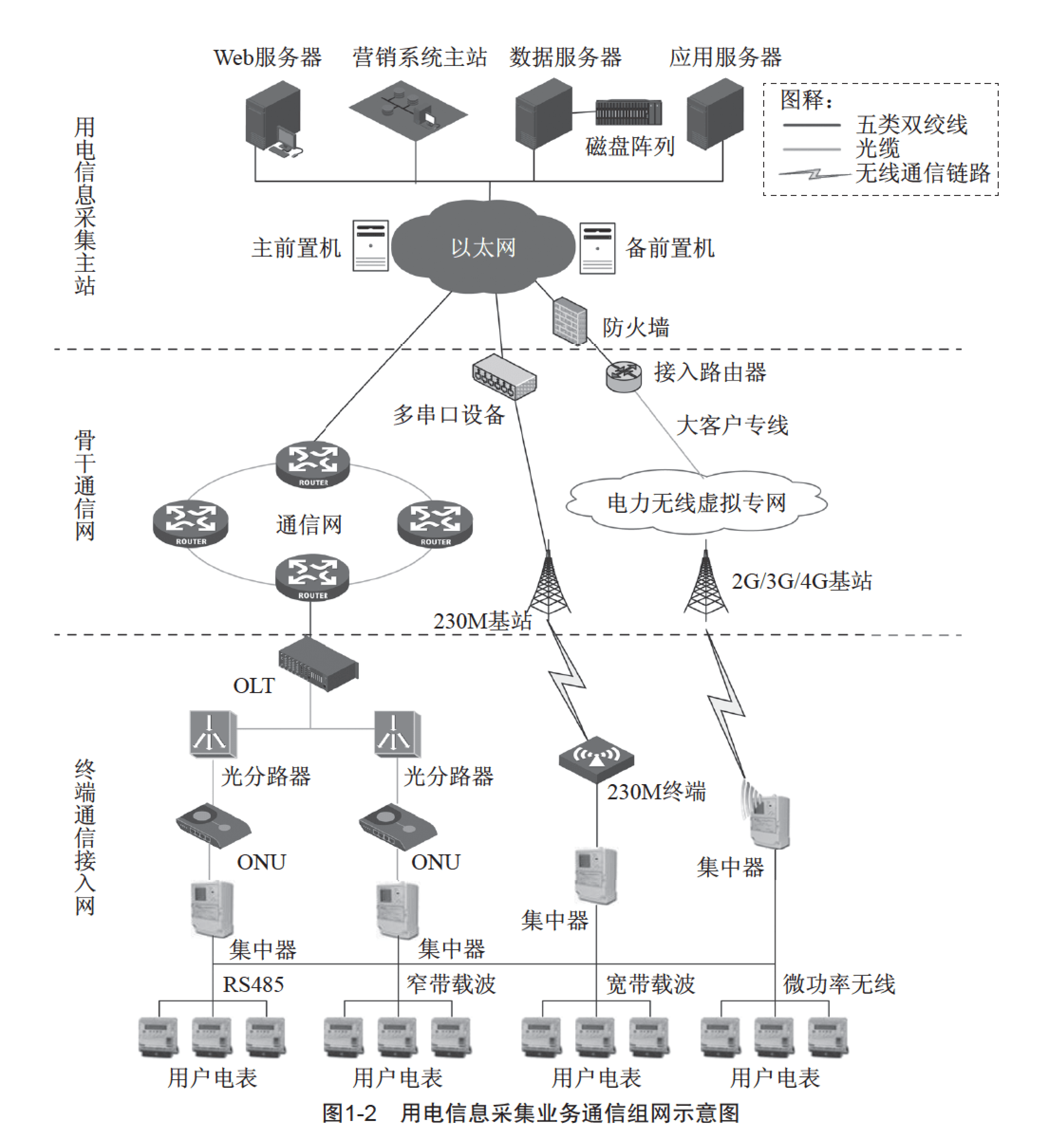


图1-2　用电信息采集业务通信组网示意图

EPON方式可采用光纤到表、光纤到集中器两种接入方式。光纤到表模式下，光纤II型集中器放置楼宇电表箱内，通过485总线串接智能电表进行电表数据采集；光纤到集中器模式下，用电信息采集ONU与I型集中器通过以太网连接。

无线专网方式下，无线终端模块安装在采集终端处（集中器、专变终端等），基站采用无线方式与无线终端模块通信，并通过光纤接入电力通信传输网，实现智能电表与采集主站的数据传输。

无线公网方式下，在采集终端侧加装SIM卡，租用运营商的GPRS、CDMA等信道，实现智能电能表通过采集终端与主站的通信。

1.1.4 分布式电源

分布式电源是指在用户所在场地或附近建设安装，运行方式以用户端自发自用为主，多余电量上网，且在配电网系统平衡调节为特征的发电设施或有电力输出的能量综合梯级利用多联供设施。分布式电源类型包括太阳能、天然气、生物质能、风能、地热能、海洋能、资源综合利用发电（含煤矿瓦斯发电）等（不含小水电）。

分布式发电站接入通信设备、线路等不考虑双重化配置，通道一般按单路配置，分布式发电站侧的通信设备型号应与电网侧保持一致性，配套的电源、配线设备以及相关的运行环境等能够保障通信设备连续、安全稳定运行的要求配置。在分布式电源密集部署且光缆易于敷设的区域，或在配电自动化光纤网络已覆盖的区域，优先选择EPON传输技术方案；在分布式电源相对分散且具备光纤网络，但不宜采用EPON技术的区域，优先选择SDH 传输技术方案；在分布式电源相对分散且光缆线路难以敷设的区域，优先选择中压电力线载波方案；在分布式电源密集且光缆敷设困难的区域，可选择无线专网方案；对10kV电压接入的分布式电源，若无控制业务需求，可选择无线公网方案，对380/220V低压接入分布式电源，优先选择无线公网方案。

目前分布式电源接入规模较小，从配电网接入的分布式电源通常按照配电站点接入，信息接入配电自动化主站；从用户侧（0.4kV）电网接入的分布式电源点，通常按照电力用户接入，应用双向电表进行电量计量，数据接入用电信息采集主站，分布式电源通信设计结构如图1-3所示。

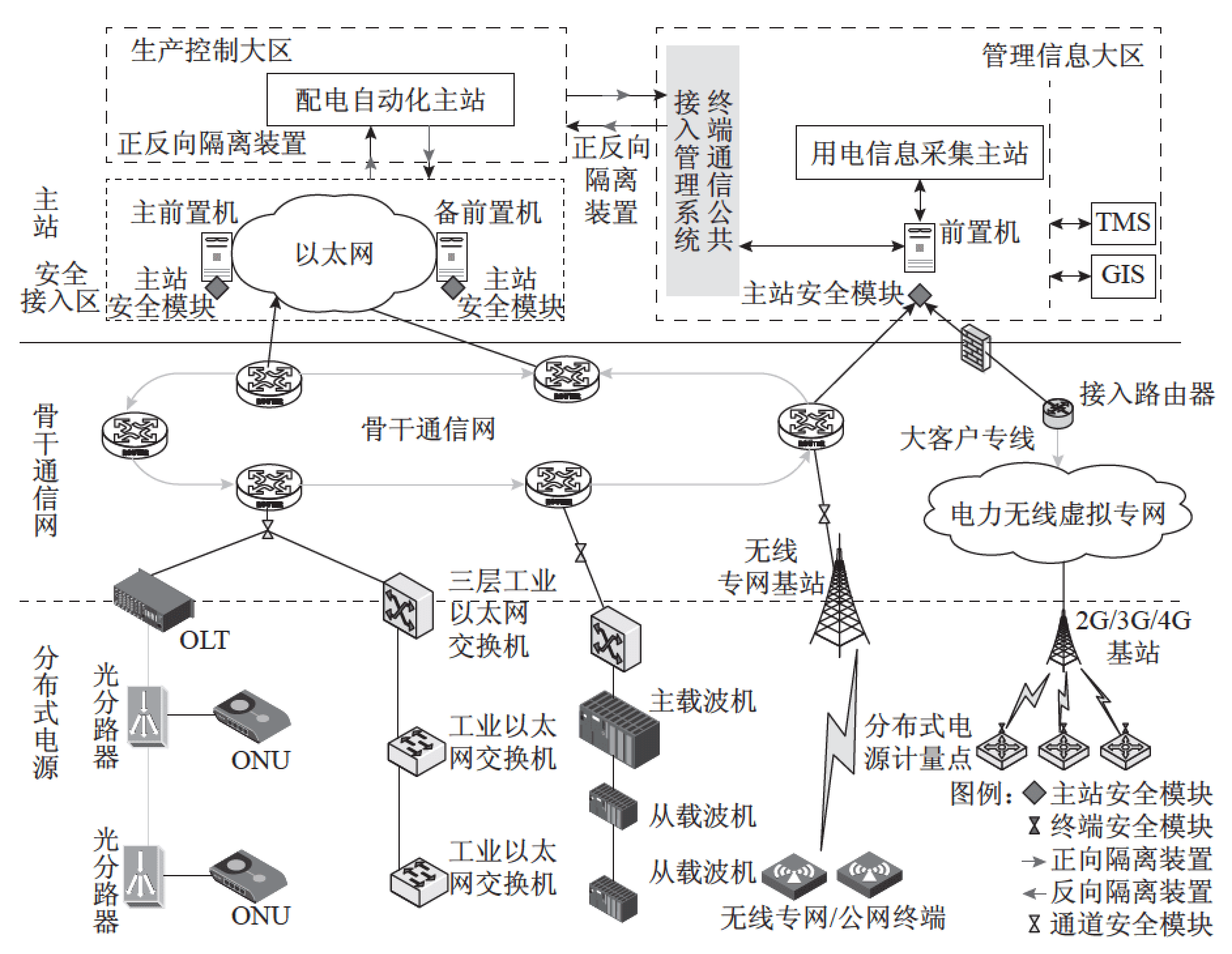


图1-3 分布式电源通信设计

1.1.5 电动汽车充电站（桩）

电动汽车充电站（桩）是指为电动汽车动力提供电能的相关设施的总称，一般包括各种集中充电站、充电桩以及车联网平台等；集中充电站含多个充电桩以及站内视频监控，集中为电动汽车提供交流电源；充电桩是采用传导方式为具有车载充电装置的电动汽车提供交流电源的专用供电装置；车联网平台部署在上海国家电网灾备中心，与客服电子商城系统、电力宝共用互联网出口；充电桩通过VPN（运营商3G/4G）将位置和状态信息上传至平台，平台通过网站和移动客户端进行发布，实现充电桩位置和状态查询、预约充电、地图导航、控制充电启停、在线充值、支付、结算等智能便捷的充电服务。

目前，集中充电站和充换电站采用“以自建电力光纤专网方式为主，租用公网运营商通信网络方式为辅”的模式，充电桩采用“充分结合终端通信网资源自建电力光纤专网，不具备终端通信网资源则租用运营商无线公网”的模式。各种通信组网方式架构如图1-4所示。

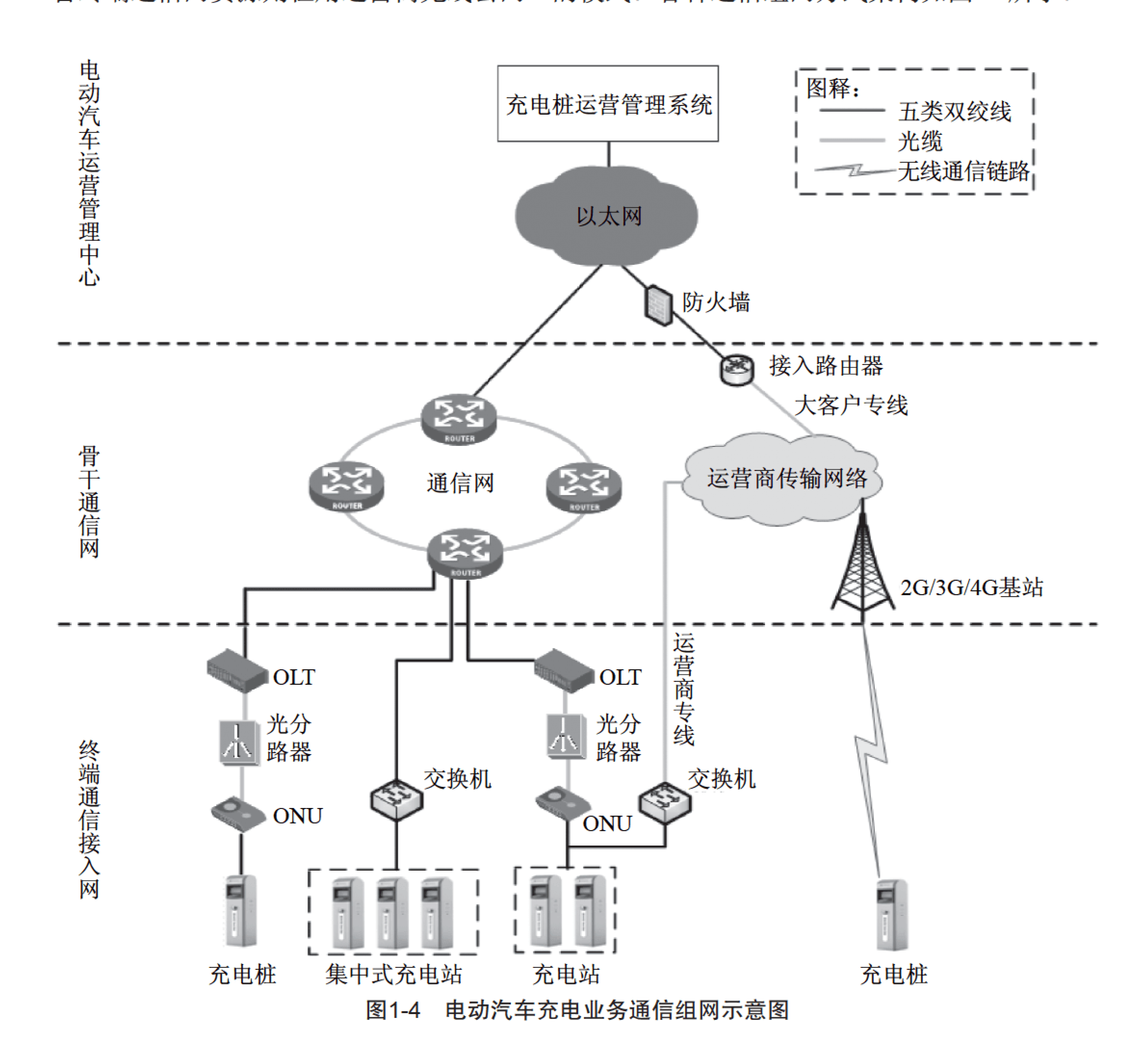


图1-4 电动汽车充电业务通信组网示意图

在终端通信接入网中，当充换电站上级电源点为变电站或具备至变电站光缆通道的开闭所时，采用自建SDH光纤专网方式就近接入变电站电力骨干通信传输网络；对于上级电源点为10kV开闭所且该开闭所不具备至变电站光缆通道的主城区充换电站以及城际高速公路充换电站时，租用运营商的专线通道。

充电桩上级电源点为10kV开闭所，且该开闭所具备至变电站光缆通道时，采用自建EPON光纤专网方式就近接入变电站电力通信传输网络；充电桩所在区域不具备终端通信接入网络资源时，采用租用运营商无线公网。

1.2　网络资源分布情况

1.2.1　光缆资源

截至2015年12月，10kV通信接入网光缆总长度达到14.94万km，新增光缆总长度97 000km。按照区域统计，华北新增光缆26 100km，华东43 800km，华中18 100km，东北2000km，西北6600km。各区域占比情况如图1-5所示。

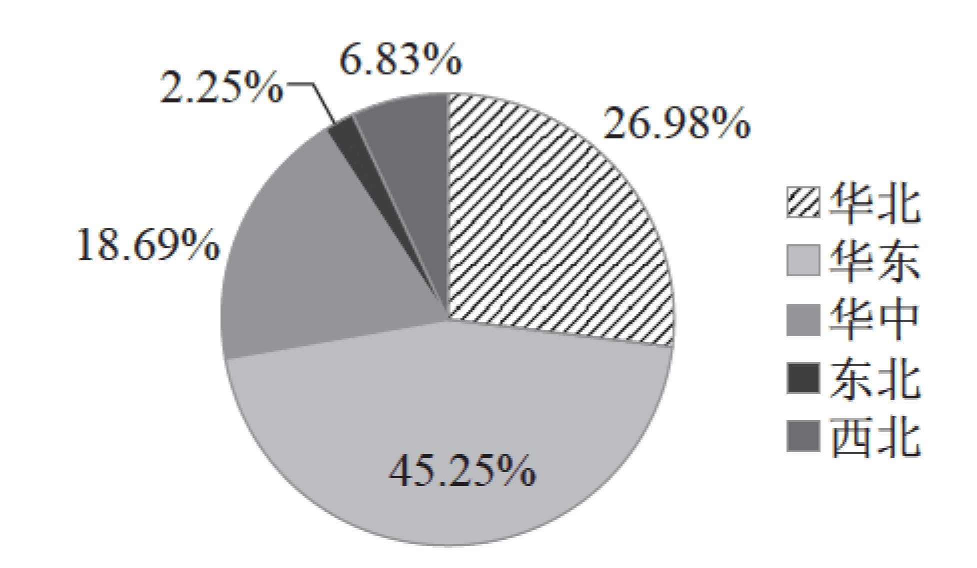


图1-5　各区域10kV接入网自建光缆长度占比

按照光缆敷设方式统计，10kV接入网主要有ADSS架空光缆、普通架空光缆、沟/隧道光缆和直埋光缆。其中ADSS架空光缆长度为34 400km，普通架空光缆长度为14 900km，沟/隧道光缆长度为42 100km，直埋光缆长度为5 600km，具体占比情况如图1-6所示。

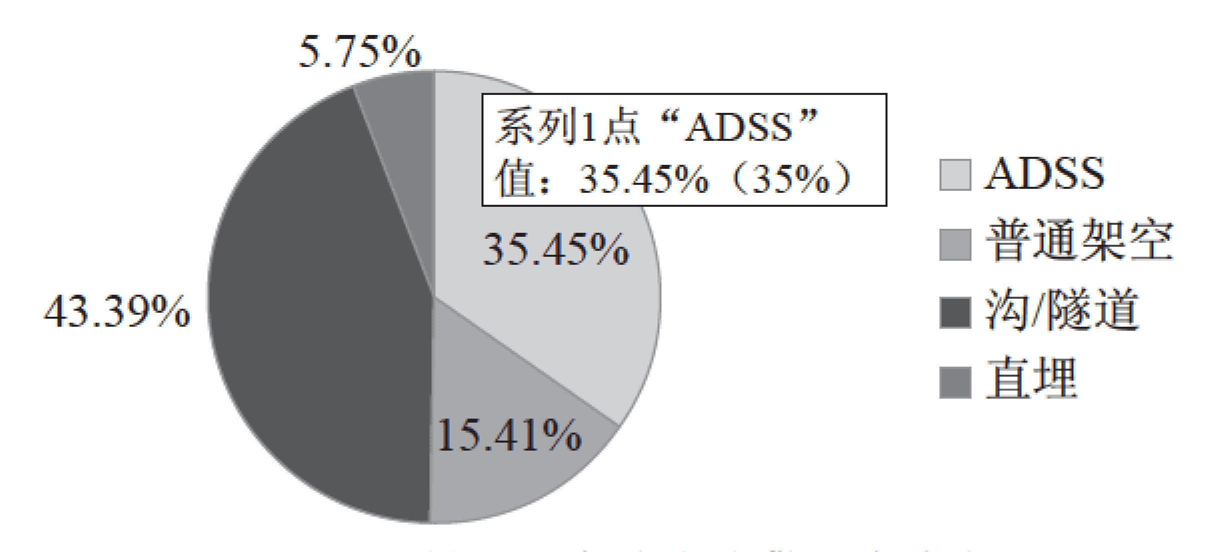


图1-6　10kV接入网自建光缆敷设方式占比

从图1-6中可以看出，沟/隧道光缆所占比例最大，直埋光缆最小。不同方式光缆敷设建设成本差异较大，实际建设中多受当地情况制约。

按照光缆纤芯数量统计，10kV接入网纤芯数量少于24芯的自建光缆长度为25 800km，纤芯数量大于或等于24而小于48的自建光缆长度为64 500km，纤芯数量大于或等于48的自建光缆长度为6700km，具体占比情况如图1-7所示。

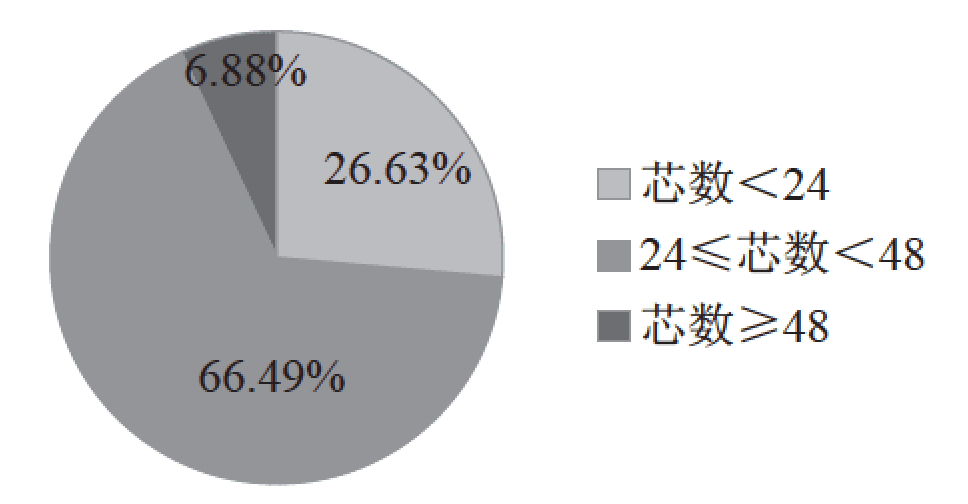


图1-7 10kV接入网自建光缆纤芯数量占比

从图1-7中可以看出，纤芯数量大于或等于24的自建光缆使用较多，可以考虑在便利的条件下，利用同光缆不同纤芯承载各项业务来提升光纤的利用率。

1.2.2 载波资源

电力线载波通信是指利用电力线作为媒介，进行语音或数据传输的一种通信方式。根据电力线缆的电压等级不同，电力线载波通信可分为高压、中压和低压电力线通信，根据使用频率范围和带宽的不同分为宽带技术和窄带技术。目前，在配电网应用的载波通信技术主要为中压电力线载波通信技术。

中压电力线载波通信是以中压（10kV）配电网电力线为传输介质的通信方式，由主载波机、从载波机、耦合器及电力线通道组成。主载波机和从载波机之间采用问答方式进行数据传输，从载波机之间不进行数据传输。载波机通过耦合器将载波信号耦合到中压配电线路上以实现数据传输，包括用于架空线路的电容耦合和用于电力线缆线路的电感耦合两种方式。

电力线载波通信技术与配电网线路高度吻合。网络拓扑为一主多从方式，主载波机一般安装在变电站或开关站，从载波机一般安装于配电站或配电设施附近。典型的电力线载波网络拓扑如图1-8所示。

其中中压PLC为电力特有通信技术，利用配电线路传输数据，载波设备外置，施工难度小。

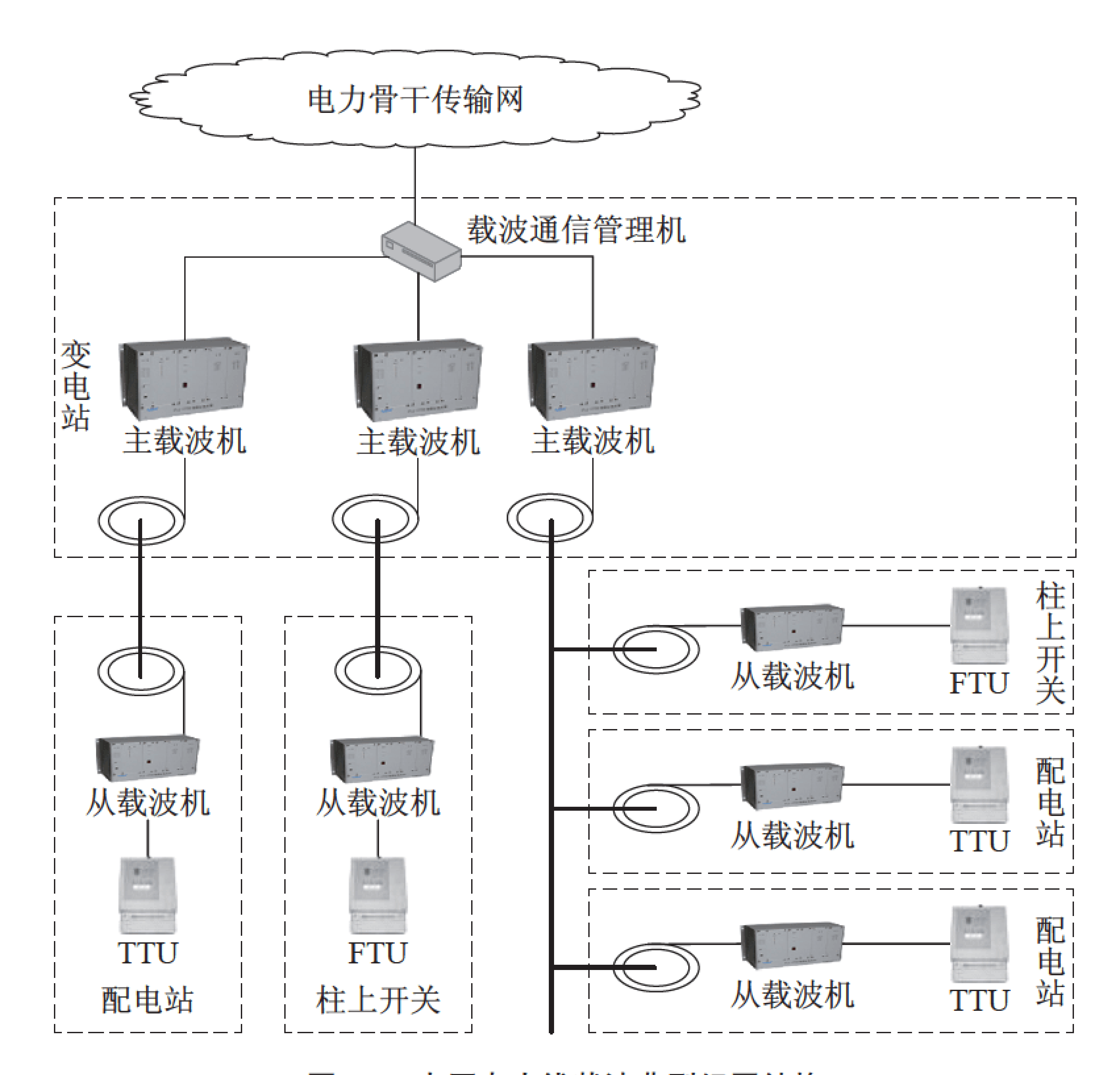


图1-8　中压电力线载波典型组网结构

1.3　无线网络资源

常用配电通信网无线技术包含移动通信无线公网（移动/联通/电信）和无线专网技术。无线专网属于自建网络，可管可控，无线公网属于租用网络，2G/3G不可管不可控，4G能够实现统一网管、数据优先等功能。无线通信网络的特点是组网灵活，不受网架结构制约，适宜进行区域覆盖。影响无线传输信道的因素有气候、地形、信号干扰等。无线传输信道具有开放性的特点，有信号被窃听和电磁恶意干扰等安全风险。无线技术具有固移结合特点，固定应用针对位置基本固定的终端，移动应用针对移动作业。

1.3.1　无线公网

我国移动通信无线公网主要由中国移动、中国电信和中国联通三家公司运营，采用的

网络制式主要为2G技术GPRS/CDMA、3G技术WCDMA/CDMA2000/TD-SCDMA和4G技术TD/FDD-LTE，其演进路线如图1-9所示。TD-SCDMA、TD-LTE是我国具有自主知识产权的无线通信系统。

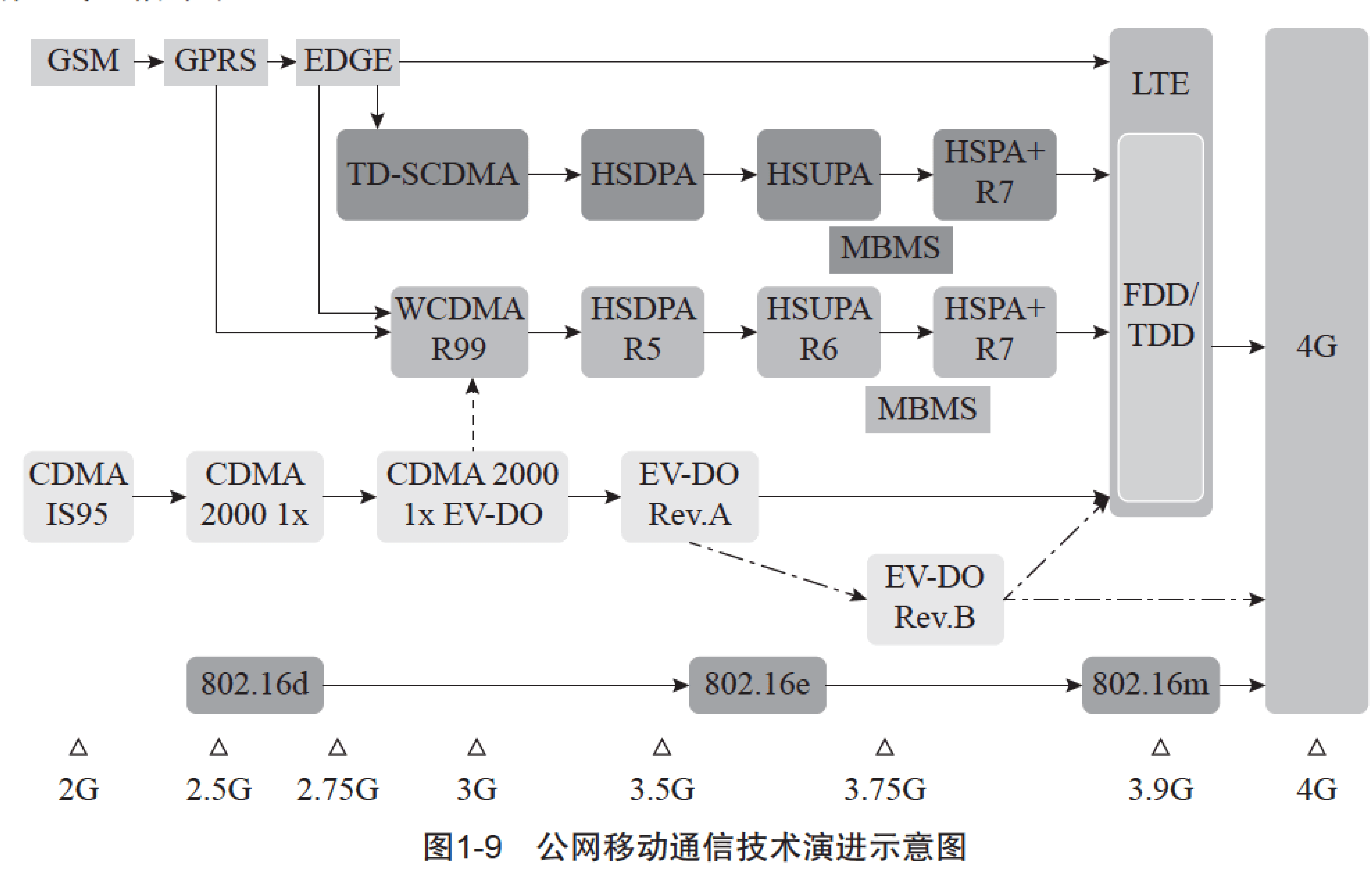


图1-9 公网移动通信技术演进示意图

GPRS是在原有的GSM移动通信系统基础之上发展起来的一种移动分组数据业务，引入了分组交换和分组传输的概念，调制方式为GMSK/8PSK；CDMA是一种扩频多址数字式通信技术，调制方式为QPSK/8PSK/16QAM；WCDMA采用直接序列扩频码分多址、频分双工方式，调制方式为QPSK/16QAM；CDMA 2000设计了两类码复用业务信道，基本信道用于传送语音、信令和低速数据，是一个可变速率信道，补充信道用以传送高速率数据；TD-SCDMA是时分双工，不需要成对的频带，关键技术包括综合寻址技术、上下行时隙配置、智能天线和动态信道分配，调制方式为QPSK/8PSK/16QAM；LTE技术采用OFDM和MIMO技术，调制方式为QPSK/16QAM/64QAM/BPSK/QPSK，TD-LTE是应用时分双工的LTE技术，支持时间和频率两个维度的链路自适应，FDD-LTE是应用频分双工的LTE技术，在分离的两个对称频率信道上，采用包交换等技术进行接收和传送。

1.3.2 无线专网

电力无线专网是指由电力公司投资建设的专属于自己的无线通信网络。无线专网组网灵活，节省有线通信线缆敷设成本，不受一次网架结构制约，适宜进行大面积覆盖，但基站选址、天线架高有一定难度。

1.4　存在的问题

1.4.1　技术体系存在的问题

通过对接入网技术体系现状的分析可知，接入网具有技术体制多、应用场景多的特点，单一通信方式难以满足不同业务、不同场景的接入需求，技术体制选择需综合考虑业务需求、技术先进性和经济成本。

目前，接入网技术体系方面，主要存在以下问题：

① 组网模式方面，业务部门针对自身业务需求分散建设通信网络，接入网与业务系统“紧耦合”，网络建设分散且重复，通信资源利用率低，部门地区存在多张接入网并存的问题。

② 技术选型方面，业务部门过度依赖设备厂商，习惯性采用先进的通信技术，设备厂商对电力业务特点了解不深，容易误导技术选型。信通部门参与业务系统（通信部分）的建设深度不够，缺乏业务与通信技术的匹配分析，导致现阶段的接入网技术政策（特别是无线通信技术）不够科学、完备，难以为新能源接入、电动汽车等新增业务提供快速、灵活、高效的技术支撑。

③ 此外，还存在配网光纤建设成本过高，无线专网频率资源不足，无线公网通道的质量难以保障，配电自动化难以兼顾系统远程通信，10kV接入网与0.4kV接入网上下衔接渠道尚未打通等问题。

1.4.2　信息安全防护存在的问题

1）配电自动化

由于具有配电自动化终端数量众多、光纤及无线等多种通信方式并存、未改造的老旧终端无法支持报文加密等特点，目前配电自动化系统中普遍选择采用单向认证的兼容模式。

配电自动化主站目前已经采取了恶意代码防护、安全加固操作系统等措施，虽然采用了基于非对称密码算法的签名来保护控制命令不被伪造或篡改，但其对外开放的服务端口依然存在着遭受以上攻击的风险，若防护措施未能有效阻断攻击或未能及时发现，则存在引发配电网一次系统事故的风险。

2）用电信息采集

用电信息采集系统主要从主站安全、终端安全、通道安全三个层面进行安全防护。用

电信息采集主站具有身份认证、信息加密等防护功能，但是缺乏隔离措施，无法禁止穿透性TCP连接。

用电信息采集设备包括集中抄表终端（集中器）、专变采集终端（专变终端）和采集器。集中器与主站通信时只做了主站对集中器的认证，集中器未认证主站；在密钥更新等流程无法有效确认主站身份，数据存在篡改等风险，不能有效确认。对于费控业务，如果主站身份被伪造可能导致用户终端被非法停复电。

用电信息采集终端部署于楼道、屋檐等易于接入计量装置的地点，一般情况下不可移动，终端处于用户侧，暴露在非法用户面前，非法用户可以通过伪造或者篡改终端的方式进入设备采集层窃取系统数据，甚至可以利用嗅探、端口扫描等攻击方式对管理信息大区产生威胁。

3）电动汽车充电站（桩）

现有的电动汽车充电站（桩）采用运营商的虚拟无线专网传入车联网服务平台，通过运营商的AAA服务器进行接入认证，在链路层未采用加密措施。

1.4.3 规划中存在的问题

电力终端通信接入网规划存在以下一些问题。

① 缺少规划协调机制，营销、配电网等专项规划没有充分衔接，接入网规划未实现统筹。

② 通信专业参与程度不够，规划深度不足，无法具体指导接入网建设发展。另外，配电网的发展受地方政府的政策影响较大，配电网规划在落实过程中存在不确定性，因而，配电网规划、营销专项规划颗粒度较粗，支撑配电自动化、用电信息采集、电动汽车及分布式电源等业务的通信网规划难以细化到具体的站点，因此配套开展建设的通信系统存在较大偏差。

③ 投资多元化导致项目分头建设，资源综合利用难度大，规划及实施成效有待提高。

1.4.4 建设中存在的问题

电力终端通信接入网建设中存在以下一些问题。

① 接入网配套通信系统建设管理薄弱，无法保证建设质量。

② 租赁规范化管理有待提升，业务保障能力不足。无线公网允许任意用户接入，对于终端仿冒、伪基站等安全问题的防护措施不足，存在安全风险；用电信息采集、配电自动化等业务终端在线率均未达到90%，不能保障业务运行、故障排查及修复要求，整体管控和服务支撑能力不足。

③ 缺乏有效的管控手段。电信运营商未提供SIM卡访问控制及网络监控等技术手段，

网管系统无法实时获取网络状态，导致业务传输时延长、一次接入成功率低、业务终端在线率不稳定、业务承载可靠性低、通道故障修复时间长等问题并且原因不明，影响服务质量进一步提高。

1.4.5　运维中存在的问题

电力终端通信接入网运维中存在以下一些问题。

① 运维职责分工不明确。运维职责界面不清晰，易造成相关部门间互相推诿、协调难度大等问题，无法有效开展现场运维工作，运维效率低，不能保障接入网的安全稳定可靠运行，最终导致无法可靠支撑各类业务的承载运行，降低各类业务的在线率、采集率、实时性、稳定性等指标。

② 运维费用缺乏标准，费用得不到保障。部分管理规定中对接入网运维方面，信通部门有运维职责但没有专项运维费用。

③ 缺少统一标准的接入网运维流程。缺少的标准流程包括运维费用申请，接入网检修，接入网消缺等流程，导致各单位无法高效地开展接入网运维工作，及时解决通信故障，无法保障接入网的可靠稳定运行。

1.5　技术条件分析

1.5.1　有线通信技术

光纤通信技术有SDH、OTN、PON、光以太网等，目前配电网应用的光纤通信技术包括EPON和工业以太网，建成的光纤专网可管可控。光缆建设应以10kV出线变电站为中心，开闭所等大型配电站点为汇聚节点，充分利用配网管（线）资源，并根据配电终端站点的地理分布结构进行光缆敷设。

1. EPON

EPON在物理层采用PON技术，在数据链路层使用以太网协议，利用PON的拓扑结构实现以太网接入，为用户提供高带宽互联网接入业务。

2. 组网方案

EPON是基于以太网的一种点到多点的光纤接入技术，它由局侧的OLT、用户侧的

ONU以及ODN组成。EPON网络的上下行数据传输过程不同：在下行方向，OLT采用广播的方式将发送的信号通过ODN到达各个ONU，ONU通过识别分组头/信元头的匹配地址来接收处理相应的数据；在上行方向采用TDMA多址接入方式，ONU发送的信号只会到达OLT，而不会到达其他ONU。

EPON追求高分光比为用户提供高带宽互联网接入服务，并不是电力通信专用技术，但EPON设备组网灵活，可与配电网线路结构很好吻合。典型的EPON拓扑如图1-10所示，OLT放在变电站机房，ONU放在开关站、环网柜和分支箱，可组成星状、总线型和手拉手结构，手拉手保护也可以连接到同一个变电站OLT不同的PON口上。

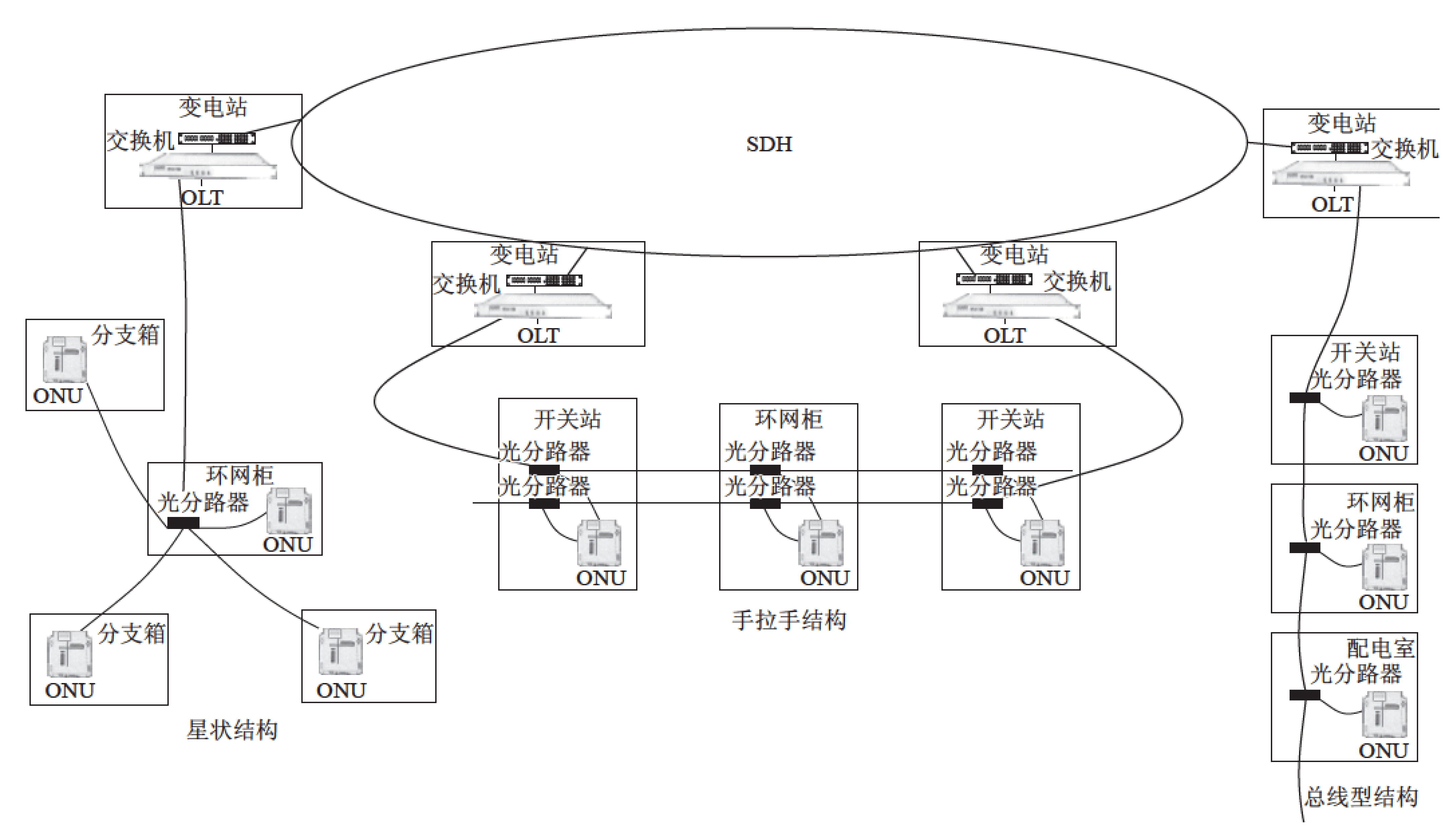


图1-10　EPON典型组网结构

根据配电自动化业务特征可知，当采用有线方式进行通信时，数据一般流向为：在变电站汇聚，经由骨干网传输至地市配电自动化系统主站。

针对配变监测终端分布地域较广、通信节点比较分散的情况，可选择采用星状结构组网，各分支箱ONU经环网柜汇聚至变电站，通过SDH传输至地市配电自动化系统主站。EPON链型组网结构契合单元辐射网络，在配电子站布放OLT，通过OLT的一个PON口级联多个POS，POS可置于每一个分段开关处（例如杆塔或者缆线分支箱），每个ONU置于FTU或者其他箱体内，满足点到多点的业务通信需求。

对于10kV变电线路而言，一般可靠性要求较高，可选择手拉手结构进行组网。EPON全链路保护组网时，其结构契合双电源手拉手网络，在两个配电子站分别布放OLT，通过两个方向利用POS进行级联延伸，每个ONU的上行链路都通过双PON扣进行链路1+1冗余保护，网络架构满足业务可靠性要求。

当变电站覆盖范围内的配电室地理位置呈近似线性分布时，可采用总线型结构组网。EPON选择线型组网时，其结构契合线网络，在配电子站布放OLT，各配电室布放ONU，

相对于手拉手网络，其光方向为单向一致。

目前，ONU一般作为外置设备。在施工难度方面，EPON敷设难度大，施工周期长，建设成本高，相比于无线网络与载波网络，施工难度大。

1）性能指标

EPON技术指标如下。

传输距离：EPON最大传输距离为20km。

带宽：EPON提供上下行对称的1.25Gbps传输速率，由于编码问题及协议开销，实际速率小于1Gbps。

时延：EPON系统的上行传输时延小于1.5ms，下行传输时延小于1ms。

对于配电自动化业务中实时性要求最高的遥控业务而言，其系统平均时延为1.5s，故EPON在实时性方面完全可以满足业务对时延的要求。变电站至台变一般在20km以内，而EPON的最大传输距离可达20km，可以满足业务对传输距离的要求。配电自动化业务带宽要求为10.2kbps，EPON可完全满足业务对带宽的要求。

EPON系统的可靠性从线路、设备和组网三个方面进行分析。对于线路可靠性而言，光纤不受电磁干扰和雷电影响，可以在自然条件恶劣的地区和电磁环境复杂的场合使用。在设备可靠性方面，配电网通信设备大多运行在户外，需保障能在恶劣天气下正常工作，并能抵抗噪声、雷电等强电磁干扰，保持稳定运行；OLT主控板1+1冗余保护、上联口双归属保护、电源冗余保护等手段可提高EPON系统的可靠性；光分路器为无源器件，设备的使用寿命长，工程施工、运行维护方便；规范规定当OLT和ONU间的光纤处于-25℃～55℃时，业务性能不应恶化或中断；针对电力应用环境，在吞吐量90%下，以太网业务的24小时丢包率应为0，野外型ONU，温度-40℃～70℃，相对湿度5%～95%，大气压力70～106kPa，防尘要求依据GB/T 4798.4—2007的4S3等级，电磁兼容符合GB/T 17626系列标准。对于网络可靠性而言，EPON系统中各个ONU与OLT设备之间通过无源光分路器采用并联方式组网，任何一个ONU或多个ONU故障或掉电，不会影响OLT和其他ONU的稳定运行，可抗多点失效；电力系统通常采用ONU双PON口设计，组网采用“手拉手”保护组网模式，光纤保护倒换时间≤100ms，如图1-11所示，当光纤发生了如图所示的两处断裂时，每个ONU还是可以和某一个OLT实现通信，保证了网络的可靠性。

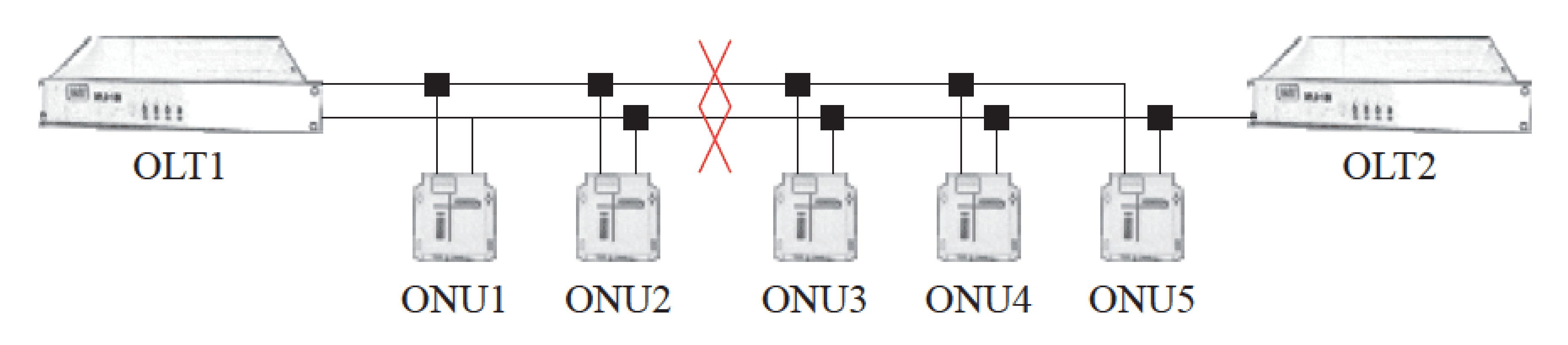


图1-11　手拉手保护方式下两处光纤断裂

配网通信系统是配网自动化的关键组成部分。要实现整个系统数据和命令的实时、稳定传输，需要可靠的通信系统作支撑。EPON由于组网灵活、扩展性强，可以很好地满足配电自动化业务的拓扑要求，同时EPON所具备的带宽高、传输距离远、损耗小、全程无

源的特性又满足了智能电网坚强可靠、经济高效、清洁环保的需求。

2）信息安全

在光纤中传输的是光信号，光信号在传输的过程中辐射非常小，并且还未有技术能够通过光辐射解析信号，因此数据通过光纤传输安全性非常高。但是在OLT和ONU的光纤组网模式中因OLT是广播数据帧，所以为了防止不可信ONU收到数据帧，在此提供三重搅动功能保护下行数据。

3）工业以太网

工业以太网技术与商业以太网（即IEEE 802.3标准）兼容，但能够满足工业控制现场的需要，可以在极端条件下（如电磁干扰、高温和机械负载等）正常工作，在工业控制领域应用广泛。工业以太网产品成熟、产业链完整，相关协议有MODBUS/TCP、ProfiNet、Ethernet/IP、HSE等。

4）组网方案

工业以太网交换机一般采用环状拓扑结构组网，在难以形成环网的应用场景可运用链式或星状组网结构，参见图1-12。

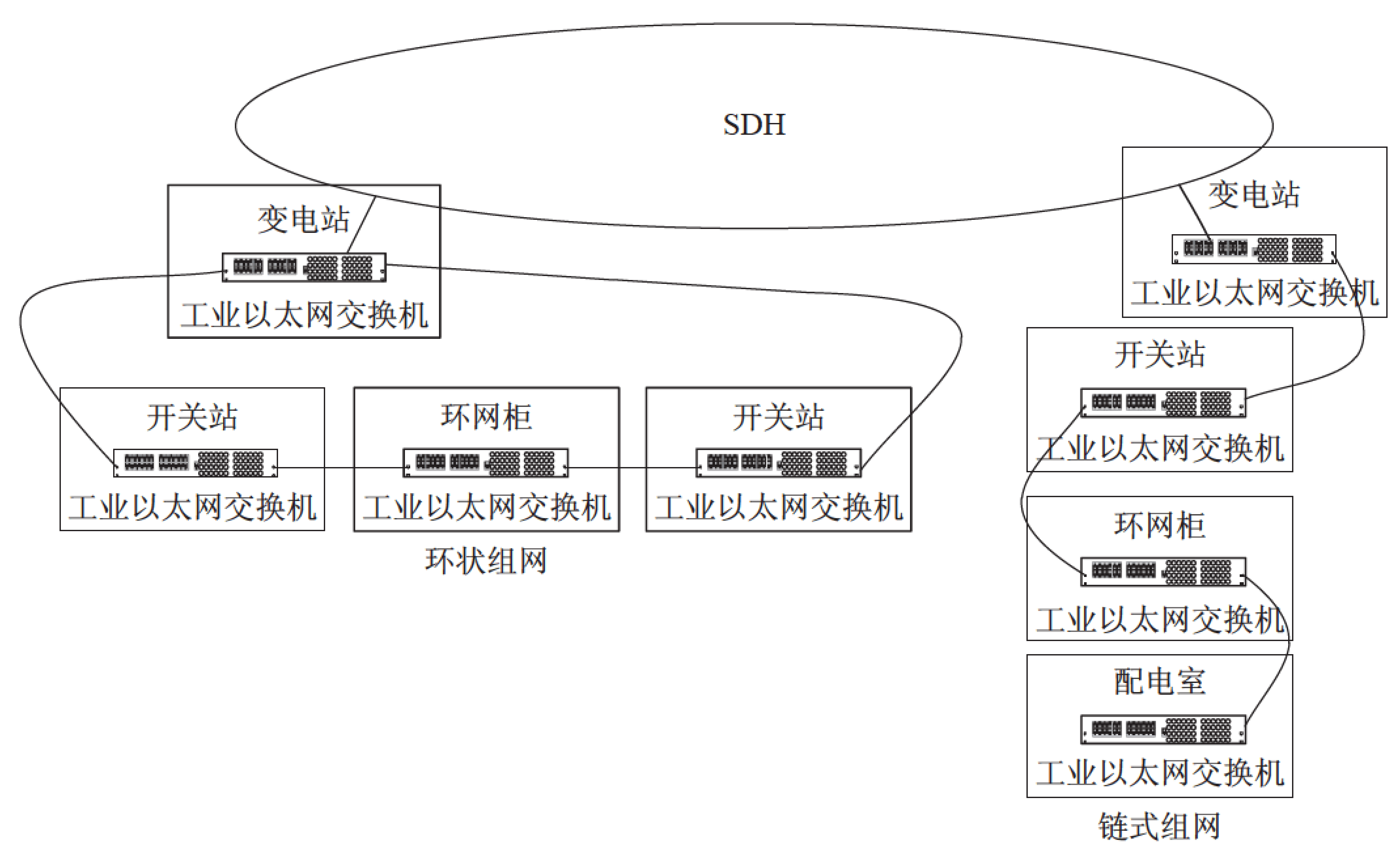


图1-12　工业以太网典型组网结构

采用链式组网时，单台交换机故障会导致其他交换机通信中断。采用环状组网方式可保证传输系统的可靠性，当环状组网发生单台设备故障（非变电站上联交换机）时，其他交换机通信不受影响。但是环网不能抗多点失效，即环上多个交换机出现故障时，会影响其他交换机的通信。

在配电自动化应用场景下，结合实际情况，尽量采用环状组网方式。环上下联节点的工业以太网交换机布放在开关站、开闭所等位置，并通过以太网接口和配电终端连接；

上联节点的工业以太网交换机一般配置在变电站内，负责收集环上所有通信终端的业务数据，并传输到骨干层通信网络。

目前，工业以太网交换机一般作为外置设备。在施工难度方面，工业以太网敷设难度大，施工周期长，建设成本高，相比于无线网络与载波网络，施工难度大。

5）性能指标

工业以太网交换机采用的元器件、接口全部达到工业级标准，性能指标如下：

传输距离：工业以太网交换机覆盖距离大于20km。

带宽：工业以太网交换机的单个端口带宽接近100/1000Mbps；环状组网时，环上各个节点共享100/1000Mbps带宽。

时延：单台交换机的时延小于0.5ms（采用如下计算办法）。

工业以太网交换机的时延 = 固有时延 + 包长/端口速率 + 排队时间。

其中，固有时延即存储转发时延，为无排队时收到最后一比特到发出第一比特的时间间隔，规范规定固有时延小于10μs；100M端口的包长/端口速率时延为5.12 ～121.44μs；交换机排队时延约为0.3ms。

采用环状组网时，以环状网20台交换机计算，总时延小于10ms。当环上单个交换机发生故障时，按照规定，恢复时间通过每个交换机的时延小于或等于50ms。

6）信息安全

以太网通信是采用电信号传输，一般采用双绞线传输，因电信号易解析，所以需要在传输数据之前进行数据加密，防止非法用户截取到关键数据。

1.5.2 电力线载波通信技术

电力线载波属于自建网络，可管可控。电力线载波根据电压主要分为两种方式：中压电力线载波和低压电力线载波。

1. 中压电力线载波

1）组网方案

中压电力线载波通信以中压（10kV）配电网电力线为传输介质的通信方式。（详见1.2.2节）

电力线载波通信技术与配电网线路高度吻合。网络拓扑为一主多从方式，主载波机一般安装在变电站或开关站，从载波机一般安装于配电站或配电设施附近。

2）性能指标

传输距离：中压窄带载波通信点对点单跳架空电力线传输距离小于10km，地埋电力电缆小于2km，通过中继组网可以覆盖整个变电覆盖区域。

带宽：传输速率10kbps～100kbps。

时延：单跳传输时延为0.3～3s。

中压宽带载波通信点对点单跳传输距离小于2km，组网后可覆盖同一变电覆盖区域；传输速率可达1Mbps，单跳传输时延为30～300ms。

可靠性：载波技术的可靠性主要从设备和通信媒质两个方面进行分析。对于设备可靠性而言，中压电力线载波设备采用工业化标准设计，可满足高温、高湿度、野外等相对恶劣的工作环境。在通信媒质可靠性方面，中压电力线载波以电力线（缆）或屏蔽层为通信介质，受电网网架结构影响较大，难以适应中压电力线结构频繁变化。同时，虽然中压配电线路阻抗较稳定，但电线分支、架空地埋混合、负载等都会对通信稳定性产生一些影响，需要采取自适应控制技术提高系统可靠性。

3）信息安全

中压电力线载波仅提供奇偶校验等功能，安全防护措施有待加强。

2. 低压电力线载波

低压载波通信将信息调制为高频信号并耦合至低压电力线路，利用0.4kV电力线路作为介质进行通信。低压电力线载波技术通常用于用户电表信息采集，由集中器、采集器及电力线通道构成。电力线载波通信一般使用3～500kHz或2～30MHz的电力线频谱资源，数据传输速率约为1kbps。在公司用电信息采集系统的本地通信技术中低压电力线载波占比超过70%。

典型的组网方式是一台集中器安装在台变侧，与每个载波通信模块保持通信，每个电表上均配有一个载波通信模块，每个载波模块自动响应或自动中继，根据电力线网络通信的不同情况实时进行自动调整。集中器上行可通过中压电力线载波通信提供上联通道，在台区配变高压侧安装中压载波从机，通过异步串口或以太网口与集中器连接，中压PLC系统提供透明传输通道至变电站接入终端通信网络。低压载波典型组网方式如图1-13所示。

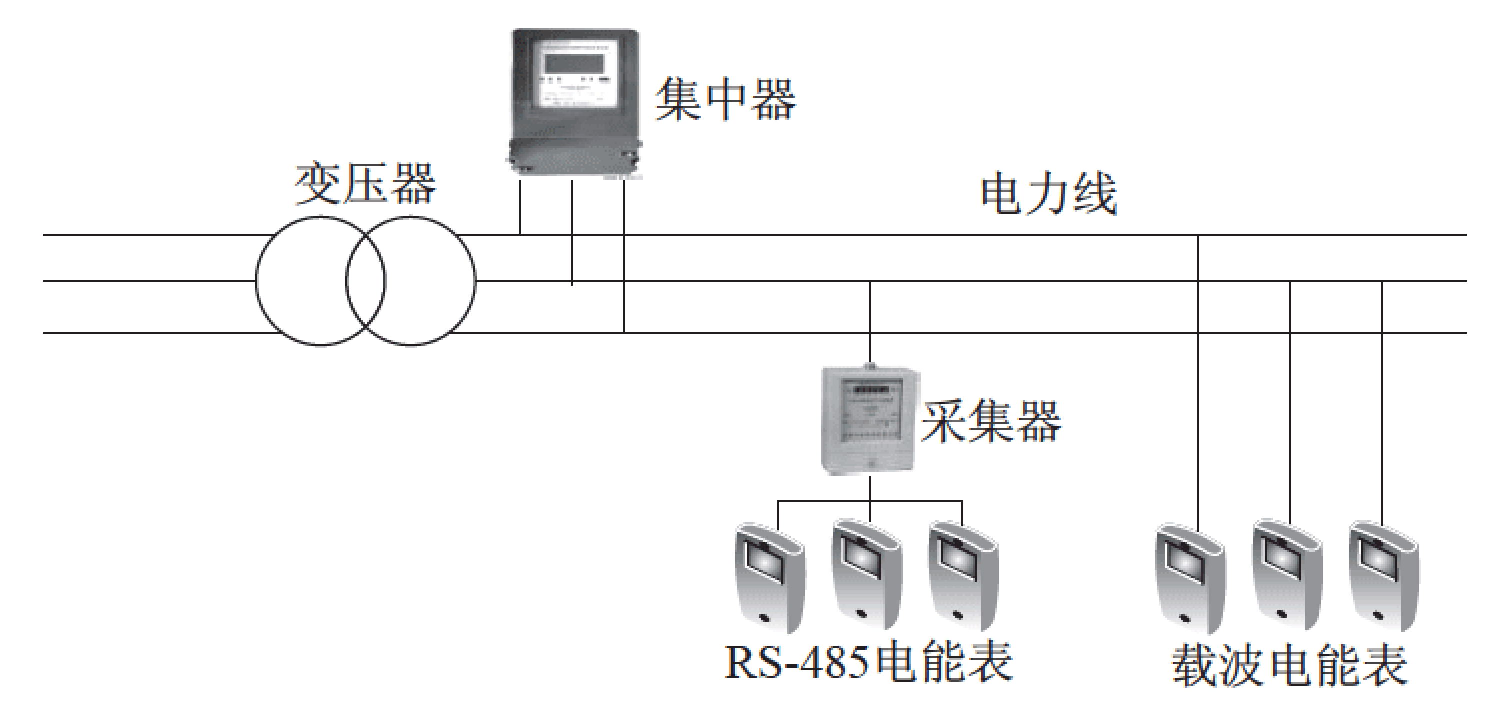


图1-13　低压载波典型组网方式

1.5.3　无线通信技术

常用配电通信网无线技术包含移动通信无线公网（移动/联通/电信）和无线专网技

术。无线专网属于自建网络，可管可控，无线公网属于租用网络，2G/3G不可管不可控，4G能够实现统一网管、数据优先等功能。无线通信网络的特点是组网灵活，不受网架结构制约，适宜进行区域覆盖。影响无线传输信道的因素有气候、地形、信号干扰等。无线传输信道具有开放性的特点，有信号被窃听和电磁恶意干扰等安全风险。无线技术具有固移结合特点，固定应用针对位置基本固定的终端，移动应用针对移动作业。

1. 无线公网

无线公网为运营商无线网络，技术标准完备，技术成熟，产业链成熟完整。目前电网对带宽与时延要求较小的业务，各网省公司仍选择以GPRS承载为主，如配电自动化业务中的非A/A+类区域的非控类业务、用电信息采集业务中的集中抄表与分布式能源计量等，考虑运营商网络性能与经济成本，部分地市选择以3G/4G网络进行承载。

1）组网方案

无线公网承载生产控制大区业务主要为配电自动化业务，配电自动化系统在各地市部署，通信终端数据通过无线公网汇聚至地市运营商，经运营商VPN专线进入地市公司配电自动化前置交换机、网关以及前置服务器，再通过正反向隔离装置传输至配电自动化主站。

无线公网由两部分构成，分别是核心网和无线接入网。核心网可以分为基站子系统、网络子系统、支撑系统三部分，其功能主要是提供用户链接、用户管理及业务承载，作为承载网络提供到外部网络的接口。无线接入网是指部分或全部采用无线电波这一传输媒质，通过基站系统连接用户移动台与交换系统的一种接入技术。交换系统完成网络主要的交换功能，管理与其他通信网络之间的通信，还包括用于移动性管理和存储用户数据的数据库；移动台是移动通信网中的用户设备，在电力应用中，终端位置基本是固定的。无线公网接入网架构示意图如图1-14所示。

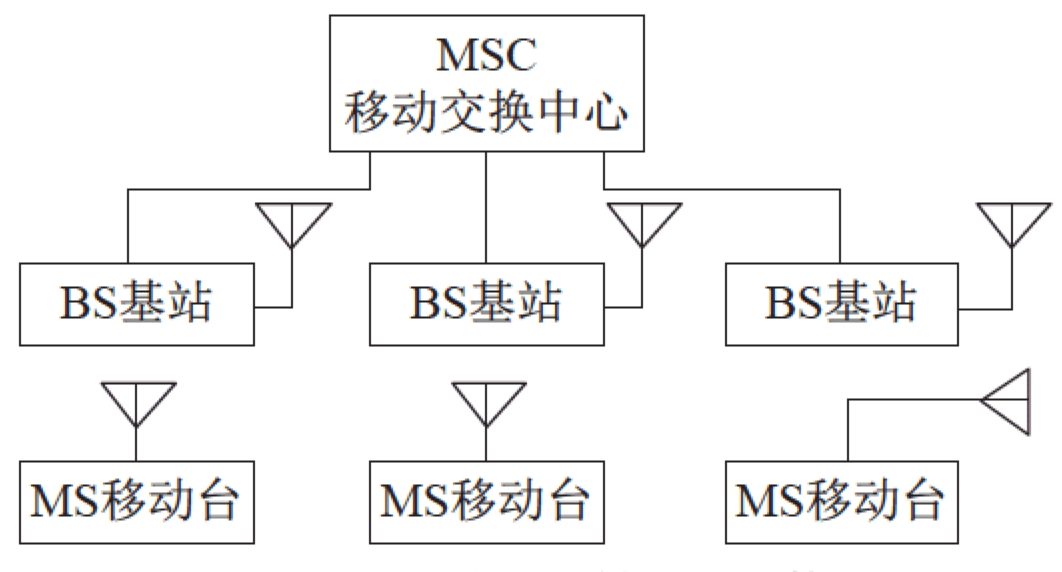


图1-14　无线公网接入网架构

无线公网模块可以设计成通用内置模块，方便安装和更换。无线公网为租用网络，不存在建设与运维成本，且无线公网在基站覆盖范围内可以实现全覆盖，若不考虑其他因素，无线公网可以满足各类配电终端的接入。

2）性能指标

无线公网的带宽是多用户共享，单用户的通信速率会受到系统容量限制，用户越多，速率越低，实时性越难以保障。2G系统平均速率为10～90kbps；3G系统平均速率为

80～700kbps；4G峰值下行速率100Mbps、上行速率50Mbps，平均速率可达5～10Mbps。对比无线公网各种不同制式的通信技术，2G带宽最小，为10kbps。据配电自动化业务带宽特征可知，传输带宽要求大于10.2kbps，故2G网络可满足业务带宽要求，3G/4G网络尚存在带宽资源浪费问题。

无线公网的传输延时为600ms～2s。据配电自动化业务实时性特征可知，对于遥控业务，系统平均时延要求小于1.5s，因而无线公网难以满足业务实时性要求。而遥测业务时延要求为30s，遥信业务时延要求为60s，无线公网可满足要求。目前二遥业务推荐优先选用无线公网。

3）信息安全

无线通信本身固有的开放性使得它更容易受到监听、滥用等安全威胁，虽然随着无线通信技术体制的演进升级，采用用户鉴权、加密等逐步增强的安全措施。GPRS安全主要包括核心网对用户的单向鉴权、空中接口加密和对用户身份信息的保护三部分；TD-SCDMA/CDMA系统相比GPRS增加了双向认证、数据完整性保护等方面的安全性；LTE采用了接入层和非接入层两层安全机制，采用更为复杂的密钥体系保护信令和数据的机密性和完整性，安全性增强。

无线公网/电力无线虚拟专网承载用电信息采集、配电自动化、分布式电源、电动汽车充电站（桩）等无线接入业务。终端采用专用SIM卡、安全TF卡/安全加密芯片，运营商内部通过APN、VPN/VPDN技术实现业务横向逻辑隔离，运营商核心网至国网公司采用有线专线接入。管理信息大区业务主要通过电力无线虚拟专网接入，在业务主站部署防火墙、安全接入平台；生产控制大区业务在业务主站部署防火墙，并设置安全接入区，通过正反向隔离装置接入主站。无线公网/电力无线虚拟专网安全防护措施符合相关规定，能够满足承载业务防护需求。

2. 无线专网

电力无线专网是指由电力公司投资建设的专属于自己的无线通信网络。

1）组网方案

典型的无线专网系统由无线终端、基站以及核心网络设备组成，如图1-15所示。无线终端放在变压器侧的设备箱、用户设备端附近或与其合为一体。

配电自动化系统以地市为单位部署，主站位于地市调度中心，配电终端沿配电线路部署，终端与主站之间点对点双向通信。无线专网组网灵活，适宜进行区域性覆盖。无线专网为电力自建网络，专网专用，核心网部署在地市，基站部署在变电站等电力场所，业务数据在基站实现汇聚，网络拓扑与电网架构大致吻合。

无线专网模块有内置模块和外置设备两种，业务终端厂家需要与内置模块厂家合作开展二次开发，现一般采用外置设备。无线专网为自建网络，施工难度相比于光纤专网较小。在基站覆盖范围内，可以实现配电终端的接入。

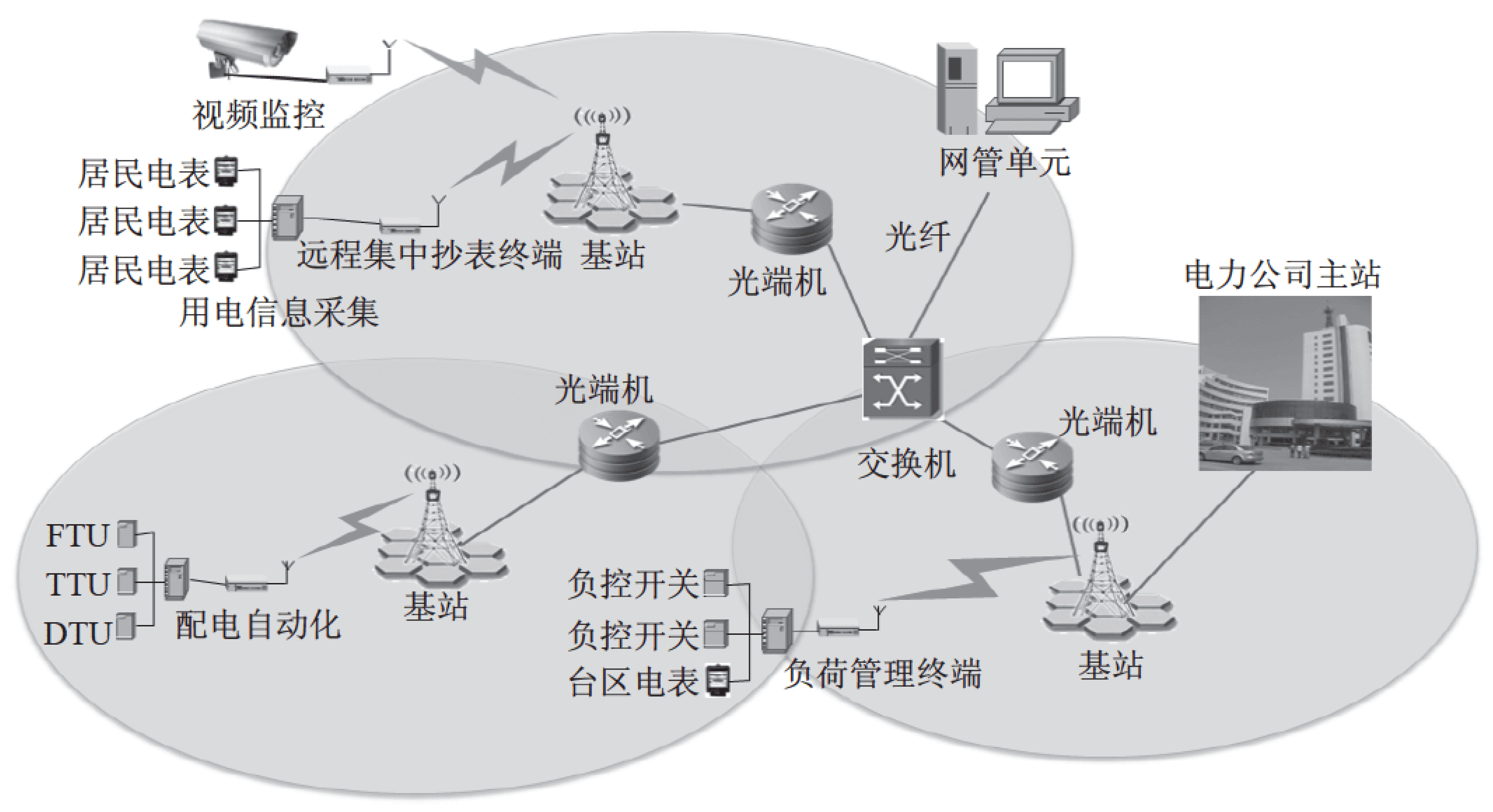


图1-15　无线专网典型组网方式

2）性能指标

（1）TD-LTE 230MHz

TD-LTE 230MHz覆盖范围市区内为3～5km，农村地区为15～20km。TD-LTE 230MHz频段共有40个离散频点共计1Mbps带宽，频谱资源不足，不能承载宽带业务；TD-LTE 230MHz系统基站最大发射功率6W，终端最大发射功率为200mW，基站支持全向/定向天线。针对电力业务上下行非对称的典型特性，TD-LTE 230MHz无线宽带通信系统按照TDD方式进行设计，根据电网实际需要进行上下行带宽配比，满足高上行比例要求上行峰值速率可达1.76Mbps，下行峰值速率为0.5Mbps，传输时延（无线终端至核心网）为100～300ms，实际速率为500kbps～1Mbps。

（2）TD-LTE 1800MHz

TD-LTE 1800MHz覆盖范围市区内为1～3km，农村地区为5～10km。TD-LTE 1800MHz采用电力、石油、交通等行业的公共频段，1800MHz频段频谱资源充足，自建无线网络能够满足覆盖范围内的宽带业务需求，系统带宽为20MHz时下行峰值吞吐量约为100Mbps，上行约为50Mbps；系统带宽为5MHz，其上行峰值速率为8.1Mbps，下行峰值速率为20Mbps，实际速率为5～10Mbps，传输时延为30～100ms。

LTE 1800MHz自建网络组网灵活，可采用多种信道编码方式以及混合重传及多基站协作技术提升网络可靠性。但TD-LTE 1800MHz系统还存在互联互通、兼容性等标准化不成熟的问题，需要建立试点应用。

3）信息安全

TD-LTE 230M/1.8G无线专网承载配电自动化、用电信息采集业务。配电自动化终端、用采终端分别采用软算法库、ESAM模块，空中接口使用基于祖冲之算法的密钥体系对信令和数据加密。配电自动化主站部署防火墙，并设置安全接入区，通过正反向隔离

装置接入主站；用电信息采集在业务终端、主站分别配置ESAM模块、密码机进行防护。230M数传电台专网专用，承载负荷控制业务，在主站应设置安全接入区，通过正反向隔离装置接入主站。

1.6 总　　结

本章梳理了电力终端通信接入网业务资源及网络资源的分布情况，分析了接入网建设与规划存在的差距，以及目前接入网普遍存在的问题。通过对接入网现有技术条件分析，得到现阶段通信技术的应用规律，明确了接入网的规划建设基础。

为缩小接入网建设与规划存在的差距，并有效解决接入网存在的问题，需在现有业务基础资源、网络资源和技术条件的基础上，对不同类型的业务进行应用需求分析，将业务和接入网技术进行匹配性分析论证，再根据业务资源分布和通信技术的特点，实现多种业务公共通信接入的统筹规划，综合评估不同业务应用场景下的适用技术，为开展终端通信接入网公共通信接入建设和运维提供技术及场景支撑。

第2章
业务应用场景与应用需求分析



2.1 业务应用场景模型分析

2.1.1 配电环节业务

配电环节业务包括配电自动化和调控一体化、配电网故障管理应用、配电网设备优化检修应用系统等，终端通信节点位于变电站开闭所环网柜柱上开关配变等设备处，随馈线走向分布，节点数量较大。调控类业务需要具备实时监测和控制功能，对通信实时性和可靠性的要求高，部分业务如配变数据采集和监测功能对通信实时性和可靠性的要求相对较低。

1. 业务介绍

终端通信接入网生产类业务包括配电自动化业务，主要实现对配电网的监测、控制和快速故障隔离，是保证电网安全、稳定运行必不可少的电网核心业务。配电自动化系统当前主要传输“三遥”业务，包括终端上传主站（上行方向）的遥测、遥信等信息采集类业务以及主站下发终端（下行方向）的常规总召、线路故障定位（定线、定段）隔离、恢复时的遥控命令，均为数据类业务。

配电是电力系统中直接与用户相连并向用户分配电能的环节，是电力系统中的重要环节，和人们生活密切相关。配电环节智能化，有助于推进配电自动化系统和配网调控一体化智能技术支持，实现对配电网的灵活调控与优化运行；有助于加强配电网生产指挥与运维管理的信息化建设，为配电网规划、运行维护和管理提供全面支撑，并实现各类应用系统的有机整合以及与调度、用电等环节的双向互动。在配电网“三流”融合与互动的基础上，智能配电网具有集成、自愈、互动、优化和兼容5个关键特征。

① 集成：通过模块化封装，实现不断的流程优化、信息整合，实现企业管理、生产管理、调度自动化与电力市场管理业务的集成，形成全面的辅助决策支持体系，支撑企业管理的规范化和精细化，不断提升电网企业的管理效率。

② 自愈：通过实时监控和计算，对电网的运行状态进行连续的在线自我评估，并采取预防性控制手段，及时发现、快速诊断和消除故障隐患；故障发生时，在没有或少量人工干预下，能够快速隔离故障、自我恢复，避免大面积停电的发生。

③ 互动：实现配电环节与批发、零售电力市场无缝衔接，支持电力交易的有效开展，实现资源的优化配置；同时通过市场交易更好地激励电力市场主体参与电网安全管理，从而提升电力系统的安全运行水平。

④ 优化：通过高级分析，实现资产规划、建设、运行维护等全寿命周期环节的优化，合理地安排设备的运行与检修，提高资产的利用效率，有效地降低运行维护成本和投资成本，减少电网损耗。

⑤ 兼容：同时适应集中发电与分散发电模式，实现与负荷侧的交互，支持风电等可再生能源的接入，扩大系统运行调节的可选资源范围，满足电网与自然环境的和谐发展。

2. 业务特征

配电业务包括配电自动化、电能质量监测、分布式电源接入（200kW以上）、配电视频监控等。其中配电自动化、电能质量监测、分布式电源接入业务位于生产控制大区，承载于通信数据网，配电视频监控业务位于管理信息大区，承载于综合数据网。业务特点如下：

① 配电业务与电力生产息息相关，对通信可靠性、实时性要求较高，对数据传输延时与丢失有严格要求，但数据流量（除视频业务外）一般不大。

② 配电业务直接服务于生产调度对通信故障率、故障修复时间有严格要求，对运维管理要求较高。

③ 配电业务位于生产控制大区，对信息安全的要求较高，要求通信信道具备较高的安全防护等级。

3. 业务场景模型

配电自动化系统是配电网的重要业务，实现现场配电终端和主站的业务数据交互。配电自动化系统部署于地市级调控中心，主站通过生产控制大区信息交互总线与调度自动化系统实现信息交互；通过信息交互总线、企业服务总线与电网GIS平台、配电网规划设计平台、营销业务系统、设备运维精益管理系统实现信息交互。建立基于以太网技术的高级配电自动化业务系统是新时期自动化业务实现的有效方式。图2-1所示为配电自动化业务场景模型。

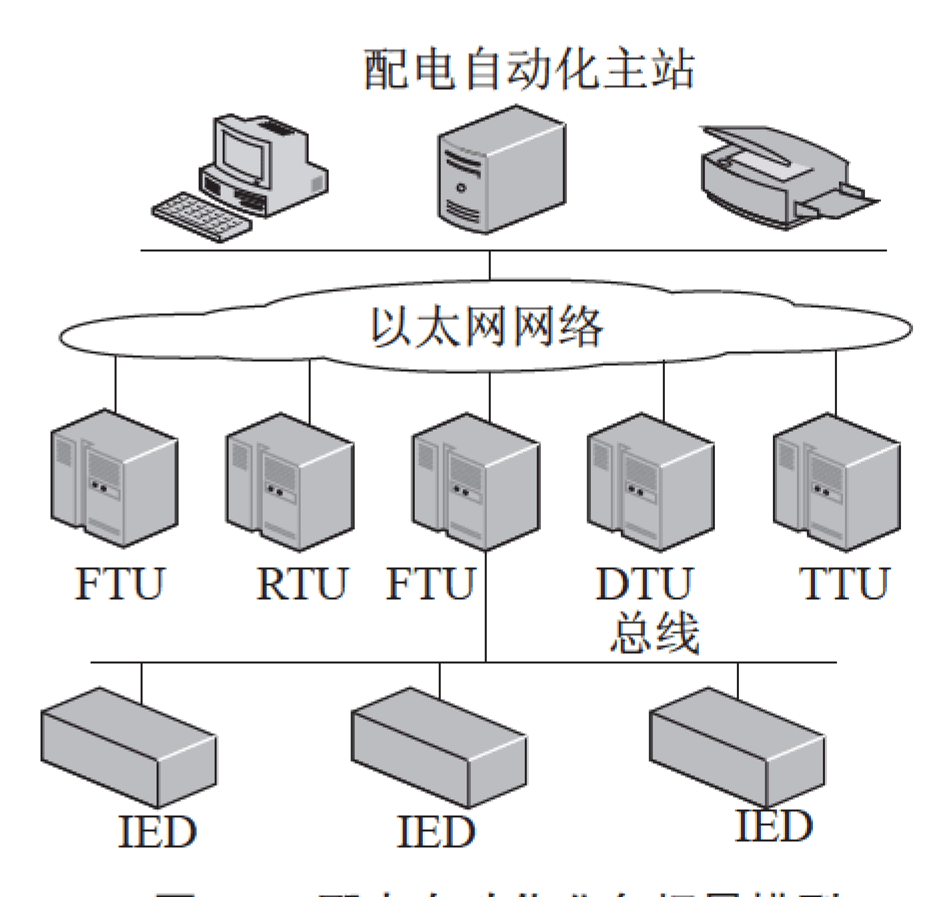


图2-1　配电自动化业务场景模型

2.1.2 用电环节业务

用电环节业务包括用电信息采集、电动汽车充电站（桩）等业务，其终端通信节点均位于用户侧，随低压用电线路走向，分布节点数量远大于配电业务，有海量的业务数据，主要业务为数据采集监测和发布，通信实时性和可靠性要求相对配电业务较低。

1. 业务介绍

随着客户的服务需求升级，客户对电网企业的服务理念、服务方式、服务内容和服务质量不断提出新的、更高的要求，除希望降低用电成本、安全可靠用电外，还希望享受更加个性化、多样化、便捷化、互动化的服务。互动服务应用依托智能电网和现代管理理念，通过传感器连接，形成绵密完整的用电和信息交互网络，并对其中信息加以整合分析，指导用户或直接进行用电方式调整，实现电力资源的最佳配置，达到降低客户用电成本、提高供电可靠性和用电效率的目的。互动服务具有以下特征：

① 智能双向结算。实现电能双向计量；自动采集客户电能量数据，电能质量数据、各种电气和状态（事件）数据，对数据进行合理性检查、分析和存储管理；实现用户与电网企业间互供电量、电费的自动结算。

② 智能化节能减排。远程监测客户侧电能质量（电压、无功、谐波等），自动进行信息发布；用户根据电价变化，远程对家用电器进行设置和控制，如低谷时开启用电设备；推动可再生能源利用、经济用电和提高能源效率。

③ 智能化需求侧管理。满足客户多元化、个性化需求。实现客户用电设备在线监测、停/投运控制，满足社会有序用电、客户经济用电的需要；实时诊断客户用电设备的健康状况，为客户提供安全用电服务。

④ 为客户用能系统提供能耗监测与能效诊断、能效项目实施效果验证等服务。

⑤ 智能分析决策。自动完成购、售电市场分析与预测，为输配电网络规划、建设提供依据；对营销指标进行统计、查询、分析、预测，为国家电价政策、节能减排政策的制定提供决策信息，为经营管理提供决策依据。

⑥ 创新商业模式。建设互动服务平台，有利于提高电能质量和供电可靠性，创新商业服务模式，提升电网与用户双向互动能力和用电增值服务水平。

2. 业务特征

用电业务包括用电信息采集、智能用电服务（智能营业厅、互动化用电、电动汽车充换电设施）等，位于管理信息大区。业务特点如下：

① 采集业务节点多，上下行流量差距较大，要求在预定时间集中采集全部用户的数据信息。

② 远程控制类业务信息随机性强，实时性要求高，信息流量小。

③ 部分扩展业务对双向实时通信有较高的要求，高端业务具备语音、数据、视频多媒体通信的特点。

3. 业务场景模型

用电信息采集系统是对电力用户的用电信息进行采集、处理和实时监控的系统，实现用电信息的自动采集、计量异常监测、电能质量监测、用电分析和管理、相关信息发布、分布式能源监控、智能用电设备的信息交互等功能。用户电量采集业务朝着全自动化、全预付费、全覆盖的方向发展，其业务场景模型如图2-2所示。

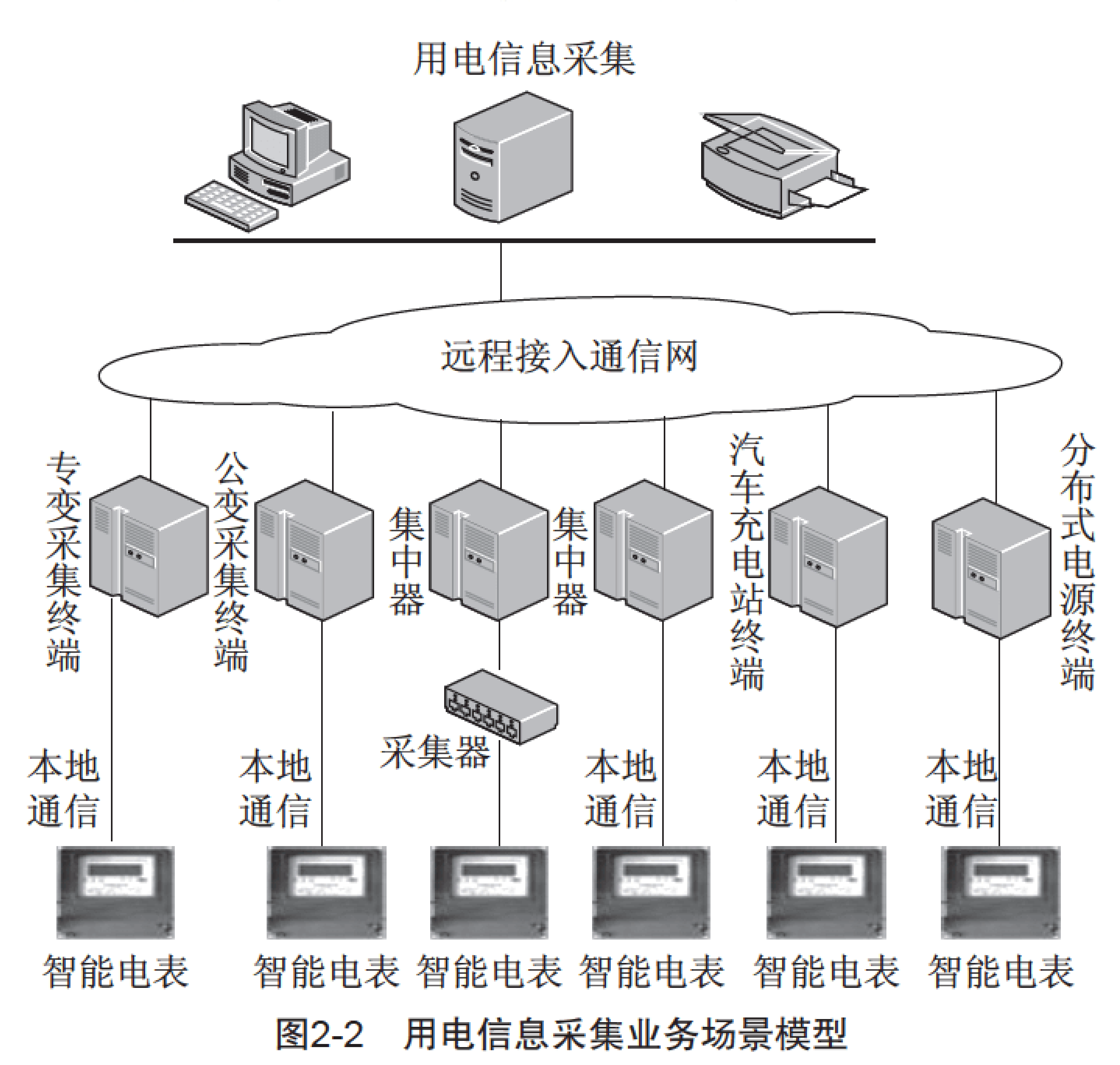


图2-2 用电信息采集业务场景模型

2.1.3 用能服务业务

1. 业务介绍

用能服务业务包括智能家居、智能营业厅、智能用电互动平台、智能用电小区楼宇等业务。用能服务包括智能化客户服务、智能化测量与控制、智能化营销业务管理与决策、智能化需求侧管理以及客户资源的开发利用，为电网与客户之间构建高效、互动的新型供用电关系，为电力客户提供多元化互动服务。

2. 业务特征

接入网实现智能用电互动平台、智能家居、实体营业厅、互动终端营业厅的视频监

控、柜台终端和自助服务终端、独立布置的自助终端和车载移动营业厅的通信接入，承载用户档案、用电信息、变更业务、缴费业务及服务管理等数据和视频业务，视频监控带宽要求最高。

3. 业务场景模型

用能服务网络是实现用户用电需求定制、多种用能策略、多样化服务等的业务网络。网络承载的业务包括语音、视频、数据业务。用电服务网络可以利用电力通信网和公共互联网，用户需求经公共互联网上传至电力服务网站，定制的服务经由电力通信网传输至用户的表计和用户终端。用能服务业务场景模型如图2-3所示。

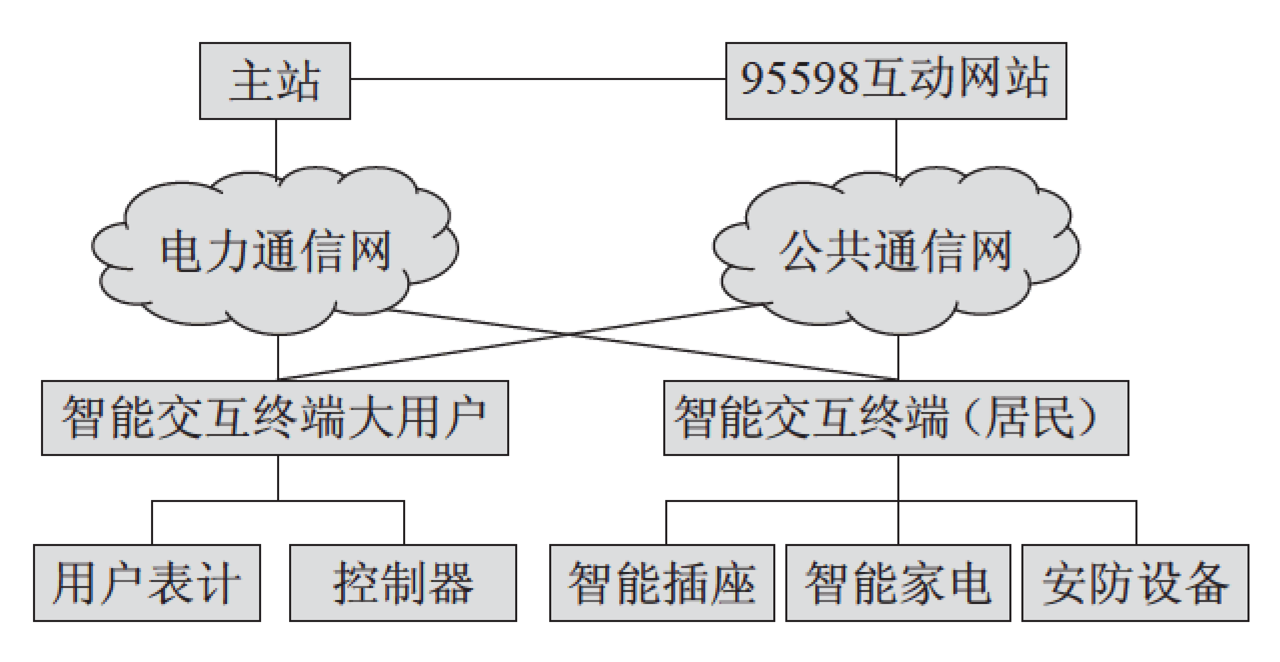


图2-3 用能服务业务场景模型

2.1.4 移动互联业务

1. 业务介绍

移动互联业务包括移动现场作业、应急抢险、移动办公、智能变电站建设等业务，能够填补原来电力系统中部分环节和场景下通信能力的不足。由于环境、成本等多重限制，在部分不便架设固定通信网络的情况下，移动互联网成为重要的通信支撑。能够使电力系统中原来的通信支撑方案在性能、成本、可靠性等方面获得提升。同时，能够实现新的更加智能化的应用，从根本上改变电力系统生成、运转和消费的模式。

2. 业务特征

移动业务是指无线专网、无线公网承载较为合适的业务，目前移动业务在全网各省公司的物资、运检、营销、基建各个环节均有应用。

物资环节移动业务主要用于仓库管理、电子商务平台等。物资环节的移动业务多借助PDA终端完成。

运检环节移动业务应用广泛，涉及生产管理、移动作业、供电电压自动采集、输变电设备在线监测、配电自动化系统、配网终端数据采集、车载GPS监控管理等。运检环节的

移动业务多借助PDA、笔记本电脑、数据采集装置、手持终端、定制终端、输电线路在线监测装置等终端完成。

营销环节移动业务主要为用电信息采集、95598门户互动（移动服务、移动作业）、一体化缴费平台等。营销环节的移动业务多借助集中器、移动POS机、负荷控制终端、专变终端、移动作业终端等完成。

在基建环节，移动业务主要集中在施工现场图像和数据采集功能，主要应用包括工程指挥、基建项目管理移动监控、基建管理信息等。

3. 业务场景模型

电力移动互联业务是电力系统应用的重要补充，主要支撑网络为自建无线网络和租赁无线公网。自建无线网络包括电力无线专网、物联网、传感网、Ad-hoc自组网等，具有自主架设、可控性强等优势。租赁无线公网可具有节省成本、覆盖面广等优势。目前，电网中的移动互联业务具有如图2-4所示的四种应用场景。

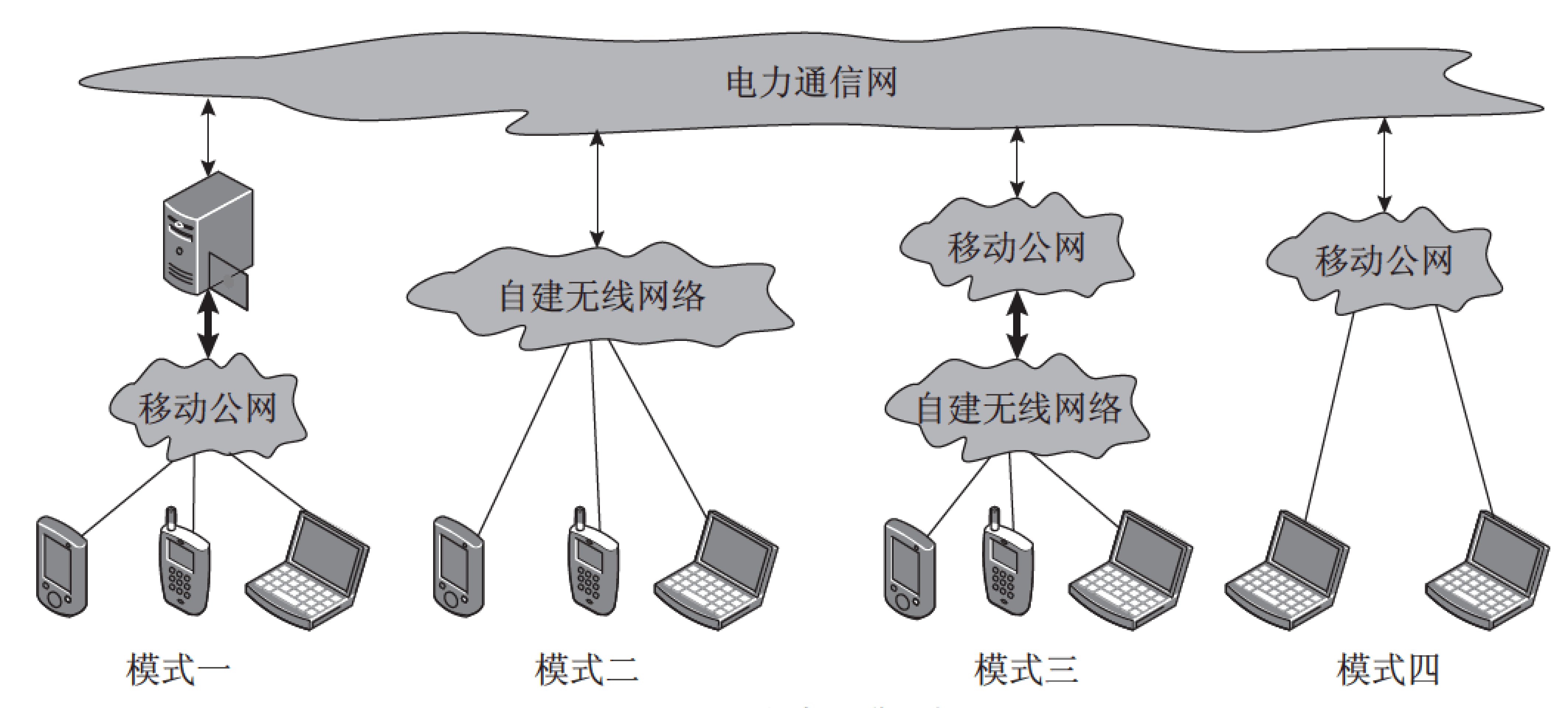


图2-4　移动互联业务

模式一为移动公网接服务器应用模式，这种模式利用移动公网作为通信支撑，可以覆盖广大的区域，实现对广域电网各种信息的采集，特点是通过公用通信设施大大扩展了电力通信能力，缺点是公网通信部分不受自主控制。

模式二为自建无线网应用模式，这种模式可利用LTE、RFID、ZigBee等技术，自己组建无线网络，补充有线专网的不足，适用于部分不便敷设有线专网或有线专网成本很高的情况。

模式三综合了自建无线网络和移动公网的优势，将两者结合起来，形成适应性更广的技术方案。突出特点是在第二种模式的基础上，进一步通过自建无线网络弥补了现有电力通信网和移动公网通信能力的不足。

模式四两端移动公网模式实际上为模式一的扩充，充分利用了移动公网覆盖面广、支持移动的特性，形成一种新的移动管理和运行的方式，可以支撑更广泛的电力业务。

基于上述的业务场景模型，在设备交互的数据类型层面，研究不同终端设备的采集数据类型、采集周期等内容，在业务处理流程方面，研究终端与上级系统之间的数据流向架构、研究业务数据流量分析、带宽需求分析、并发性要求、实时性要求、安全性要求与可靠性要求分析等内容，也成为目前建设业务所进行考量的标准。

2.2 业务需求分析

2.2.1 配电环节业务

1. 配电自动化

我国的配电自动化覆盖水平仍然较低。限制配电自动化系统规模建设的因素主要集中在配电网自身和配电网配套通信系统两个方面。对于配电网自身，配电自动化系统建设需要满足两个基本条件：一个是配电网网架结构足够坚强（实现三分段、三联络），实施配电自动化建设与改造的区域供电可靠性指标应达到99.9%以上；另一个是配电网负荷相对较低（60%～70%）。对于配电网配套通信系统，配电自动化系统建设受到两个因素影响：一是配电网配套通信系统可靠性；二是配电网配套通信系统供电。

架空线路上配电自动化终端为安装在柱上开关等处的馈线终端（FTU）。配套通信终端安装于架空线路杆塔上，容易受到天气、环境等因素影响，同时通信终端供电仅能依靠PT（电压互感器）/CT（电流互感器）取能（PT/CT一般作为独立供电设备，也可以集成在FTU中）、超级电容和蓄电池，通信可靠性难以保障，因此架空线路故障隔离一般采取就地控制方式，不采取遥控方式。

电缆线路上配电自动化终端为安装于配电网开关站、配电室、环网单元、箱式变电站等处的站所终端（DTU）。配套通信设备一般位于地面柜内或机房，不易受到天气、外界环境等因素影响，同时通信终端供电方面，环网柜中与DTU共用蓄电池（3～5年即需更换，机房内7～8年更换），通信可靠性可以得到较好保障，因此电缆线路故障隔离可以采用遥控方式。

目前三遥业务主要采用光纤通信方式，仅有个别的小规模尝试采用无线公网承载三遥。从时延结果看，使用无线公网时延波动较大，延时从几秒到几十秒、几分钟；从终端在线率看，光纤通信方式实际效果与公网无线相比无十分明显的提升，分析原因为EPON通信系统存在整条链路出现故障的现象，再加上通信维护力量的不到位、不及时因素，拉低了终端在线率。例如，没有建立手拉手结构时，某个PON口损坏或光缆中断会导致下连

的所有终端皆失效。

考虑配电自动化系统的技术经济效益，应合理选取二遥/三遥功能，对于可以采用本地控制、配置“二遥”或故障指示器的区域，可以采用除光纤之外的其他有效通信方式。

四遥和五遥是在一遥、二遥和三遥的基础上逐步发展而来的，主要用于发电厂和变电站，基本不用于配电自动化系统；四遥在三遥的基础上多了遥调（Tele-Controlling，TC）即远程调节，电力系统调度中心远程调节调度范围内的发电厂、变电站中电气设备的各种参数；五遥在四遥的基础上多了遥视（Tele-Viewing，TV），以视频传输的方式将电力调度范围内的发电厂、变电站中电器元件的状况传送给调度中心。

1）配电自动化系统架构

配电自动化系统由配电自动化系统主站、配电自动化系统子站、信息交换总线、配电自动化终端等组成，系统架构如图2-5所示。配电自动化系统以一次网架和设备为基础，综合利用计算机、信息及通信等技术，并通过与相关应用系统的信息集成，实现对配电网的监测、控制和快速故障隔离。配电自动化系统是实现配电网运行监视和控制的自动化系统，具备配电SCADA（Supervisory Control And Data Acquisition）、馈线自动化、故障处理、分析应用及与相关应用系统互连等功能。

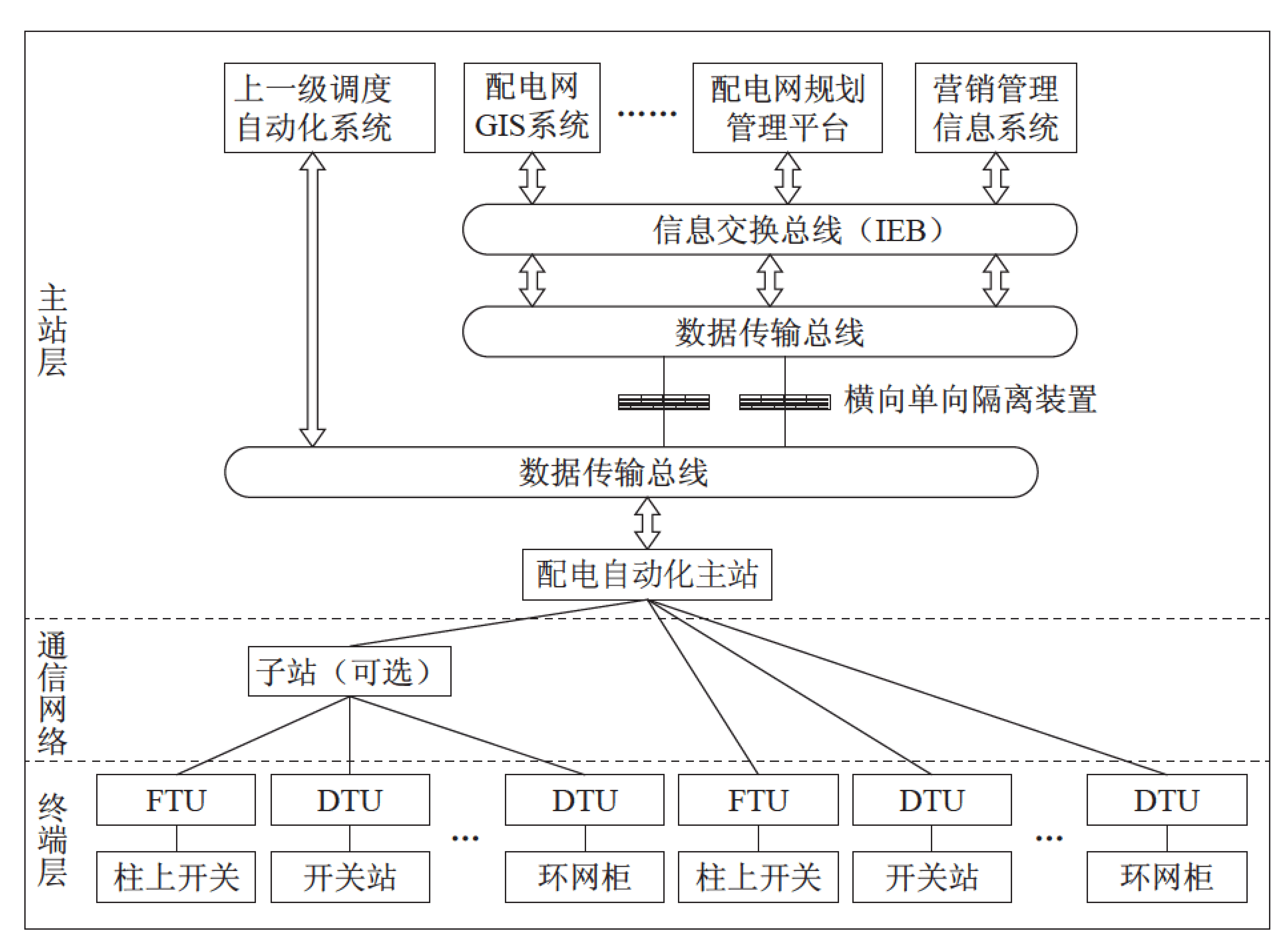


图2-5　配电自动化系统构成

2）配电自动化通信需求

（1）通信协议及数据类型

配电自动化数据传输采用的通信规约包括IEC101和IEC104规约两种。IEC101规约

主要用于串口传输（含起始字节、校验字节、结尾字节）；IEC104规约适用于以太网传输（只有起始字节，无校验字节和结尾字节，以太网底层传输自带校验，以255B为1个包）。配电自动化数据包括初始化数据帧6B、系统对时数据帧22B、心跳帧6B，主站总召帧16B；主站与终端间常规交互数据帧头12B，其余数据长度随遥信、遥测、遥控点位数量变化而变化。

（2）带宽及采集间隔

根据调研情况，配电自动化主站对终端的常规总召频率可根据需要设置为1～60min每次；心跳数据帧30s一次；主站与终端的时间隔可设置，一般每小时一次；遥信、遥控方面，主站下发命令或终端设备因突发事件主动上传数据时，频率不固定。遥测方面，采用光纤通信方式时，配电终端一般设置为电压变化1V，电流变化10mA往主站上送一次数据；采用无线通信方式时，配电终端一般设置为电压波动1V，电流波动50mA往主站上送一次数据。

单个配电终端接入速率要求为光纤专网大于或等于19.2kbps，其他方式大于或等于2.4kbps（单个配电终端接入速率要求来源为：配电终端串口可选速率为1200bps、2400bps、9600bps、19 200bps，2400bps为常用速率，考虑光纤带宽大，因此选择最大速率要求）。根据调研情况，配电自动化终端传输一包数据255B需耗时200ms，按实时传输计算（不考虑存储转发），为避免排队时延，带宽应高于10.2kbps。

（3）传输距离

配电自动化终端至主站包含两部分，终端至变电站和变电站至主站的距离，其中变电站至主站经过骨干网上传，终端至变电站的距离在采用有线方式的情况下，A+类区域约为3～5km，A、B类区域约为5～10km，C、D、E类区域约为10～20km，部分区域达到数十公里。

（4）可靠性

配电终端月平均在线率≥95%；遥控使用率≥90%；遥控成功率≥98%；遥信动作正确率≥95%。对通信系统可靠性需求较高的区域，网架结构采取冗余配置。

2. 配网抢修

1）业务概况

配网抢修作为配电生产常规性重要工作，具有全天候故障响应、直接面对用户、故障情况多样、作业环境复杂等特点。抢修模式包括主动抢修（智能电表停电信息上送）与被动抢修（客户报修）两种。

配网抢修具体包括两个层面：一是对配网调度发现线路故障信息或95598报修信息的快速、精准响应，在此过程中抢修班通过移动终端（PDA等）从后台获取故障区域的详细信息，精确到杆塔、线路、终端，提高抢修效率；二是配网抢修指挥人员与现场抢修人员的互动，具体包括配网抢修指挥人员对现场抢修人员的远程指挥、疑难问题远程视频会

诊，以及现场抢修人员远程反馈抢修结果。

2）通信需求

配电抢修业务用于采集和传输配电故障现场的语音、图像、视频信息，传输速率需求约为4Mbps，时延要求为百毫秒级。

3. 配电设备/环境状态监测

1）业务概况

配电设备/环境状态监测面向配电状态检修业务，状态监测作为技术手段，目前主要功能偏重测温（环网柜、配电室、线路等）。监测终端功能主要包括站房（环网柜、配电室等）测温、带电检测等，以及少量的配电线路状态监测。

2）通信需求

业务对带宽要求较低，实时性要求不高，通信网络一般独立建设，通信方式以无线公网为主，也可采用已建配电自动化网络。单个接入点的速率需求约为几千比特每秒，传输时延为秒级。

4. 分布式电源接入监控系统

1）业务概况

分布式电源接入监控系统由分布式电源监控系统主站（可作为功能模块集成在高级配电自动化系统主站）、分布式电源监控终端和通信系统组成。分布式电源接入监控主站具备与调度自动化、用电信息采集等系统信息交互功能，是监控系统监控和管理的中心；分布式电源监控终端是安装在分布式电源侧的自动化装置，根据分布式电源容量、接入位置及接入配电网的电压等级，配置不同功能。

2）通信需求

为适应新能源和分布式电源接入，需新建改造110kV线路4512km、35kV变电容量391万kVA、35kV线路2912km、10kV配变容量432万kVA、10kV线路8469km、380/220V线路5853km。

（1）数据类型及数据流向

分布式电源监控终端与主站系统之间通信为点对点通信，35/10kV分布式电源与主站之间传输的数据包括电能质量监测、测控和关口计量信息，电能质量监测和测控信息通过终端通信接入网和地市骨干通信网传到主站，关口计量信息为用电信息采集的一部分，直接传到用电信息采集主站。380/220V分布式电源仅有关口计量信息，关口计量信息为用电信息采集的一部分，通过无线虚拟专网直接传到用电信息采集主站。

（2）带宽及采集间隔

分布式电源接入监控按每秒上传1次数据计算，根据每个接入终端点上送32点遥测，16点遥信，1点遥控计算信息量，总数据量为444B，合计流量为3.5kbps。

（3）传输距离

35kV分布式电源接入电网形式以通过35kV电压等专线接入220/110kV变电站母线距离最长，一般不超过20km。10kV分布式电源接入电网形式以通过10kV电压等级专线接入110/66/35kV变电站母线距离最长，与配电自动化业务接入距离一致。0.4kV分布式电源接入电网形式以专线接入380V配电网最长，通常不超过500m。

（4）可靠性

分布式电源业务的可靠性需求如表2-1所示。

表2-1　分布式电源接入监控系统可靠性指标

性　　能	指　　标	
遥测	综合误控率/%	≤1.5
遥信	正确率/%	≥99.9
遥控	正确率/%	100
子站、监控终端无故障	平均无故障时间/h	≥26000
系统可用	可用率/%	≥99.9

（5）信息安全要求

分布式电源接入时，应满足“安全分区、网络专用、横向隔离、纵向认证”的二次安全防护总体原则，需配置相应的安全防护设备。

（6）其他要求

分布式电源监控终端由于部署环境较差，电磁环境复杂，最好采用工业级设备。分布式电源监控终端部署在电网并网点或接入点等位置，同时需要部署电网保护等设备，通信终端随之部署于专用机柜，属于室内部署。嵌入集中器的通信模块供电依靠集中器，需要具备低功耗、大功率等特点。独立的通信终端，在满足通信需求的前提下，功耗越小越好。为了后期运行维护需要，分布式电源监控终端通信设备均要求可管可控，方便管理者进行远程通信配置，判断故障点位置。

5. 电能质量监测

1）业务概况

电能质量监测系统按照分层、分布式结构组建，包括监测设备层、服务层和客户层，不同监测系统通过服务层互联来实现数据交换。

其中，监测设备层具有数据采集功能，以统一格式将数据传输至服务层，由电能质量监测终端（以下简称监测终端）和适配单元（可选）构成。服务层具有监测数据管理与分析、系统维护、权限管理等功能，是监测设备层、客户层之间数据交互的纽带，由若干个服务站构成。客户层具有监测数据访问、浏览、查询等功能，通过网络访问服务层。

2）通信需求

电能质量监测系统数据传输通道需求如表2-2所示。

表2-2　电能质量监测系统数据传输通道需求

项　　目	模 拟 通 道	数 字 通 道
传输速率	＞9600bps	＞1Mbps
工作方式	双工，有主备用通道时，可由服务层控制自动或手动切换	双工、点对点传输时应有备用通道，可由服务站控制自动切换；网络传输时应能自动封闭环状结构的故障段
比特差错率	＜10^{-5}	数字微波应≤10^{-6}，光纤通道应≤10^{-9}
其他要求	接收电平：-40～0dB； 发送电平：0～20dB	通道接口应符合ITU-T及ISO有关接口标准

2.2.2　用电环节业务

1. 用电信息采集

1）业务概况

用电信息采集业务用户主要包括大型专变用户、中小型专变用户、三相一般工商业用户、单相一般工商业用户、居民用户、公用配变。用电信息采集系统物理架构由采集主站、通信通道和终端组成，功能包括系统数据采集、数据管理、控制、综合应用、运行维护管理、系统接口等。用电信息采集系统物理架构如图2-6所示。

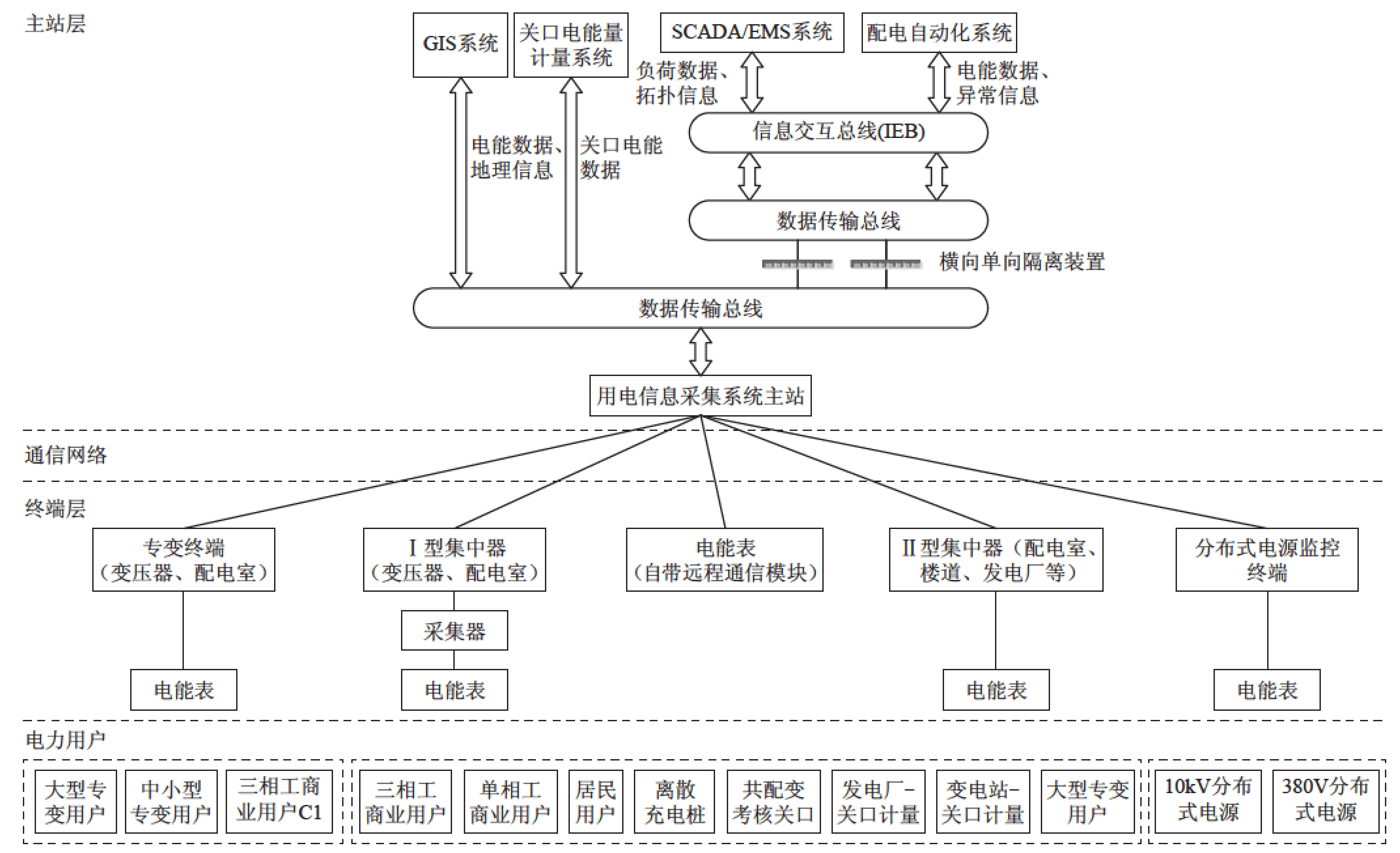


图2-6　用电信息采集系统物理架构图

2）通信需求

（1）数据类型及数据流向

用电信息采集主站与采集终端之间采用GB/T 18657.1—2002的6.2.4条FT1.2异步式传输帧格式，数据帧由起始字符（68H）、报文头（固定长度）、起始字符（68H）、控制域C、地址域A、链路用户数据、校验和CS、结束字符（16H）组成。

用电信息采集的数据流向包括上行和下行两类。上行数据流是指低压工商业、居民用户和公配变用户的电能表数据经过采集器（可选）上传到集中器，集中器经上行通信通道传到用电信息采集系统主站；专变用户电能表的数据上传到专变终端，专变终端经上行通道传到用电信息采集系统主站。用电信息采集的下行数据流是指用电信息采集系统主站通过集中器和专变终端下发指令到电能表，开展跳合闸、安全认证命令等控制业务。数据流向如图2-7所示。

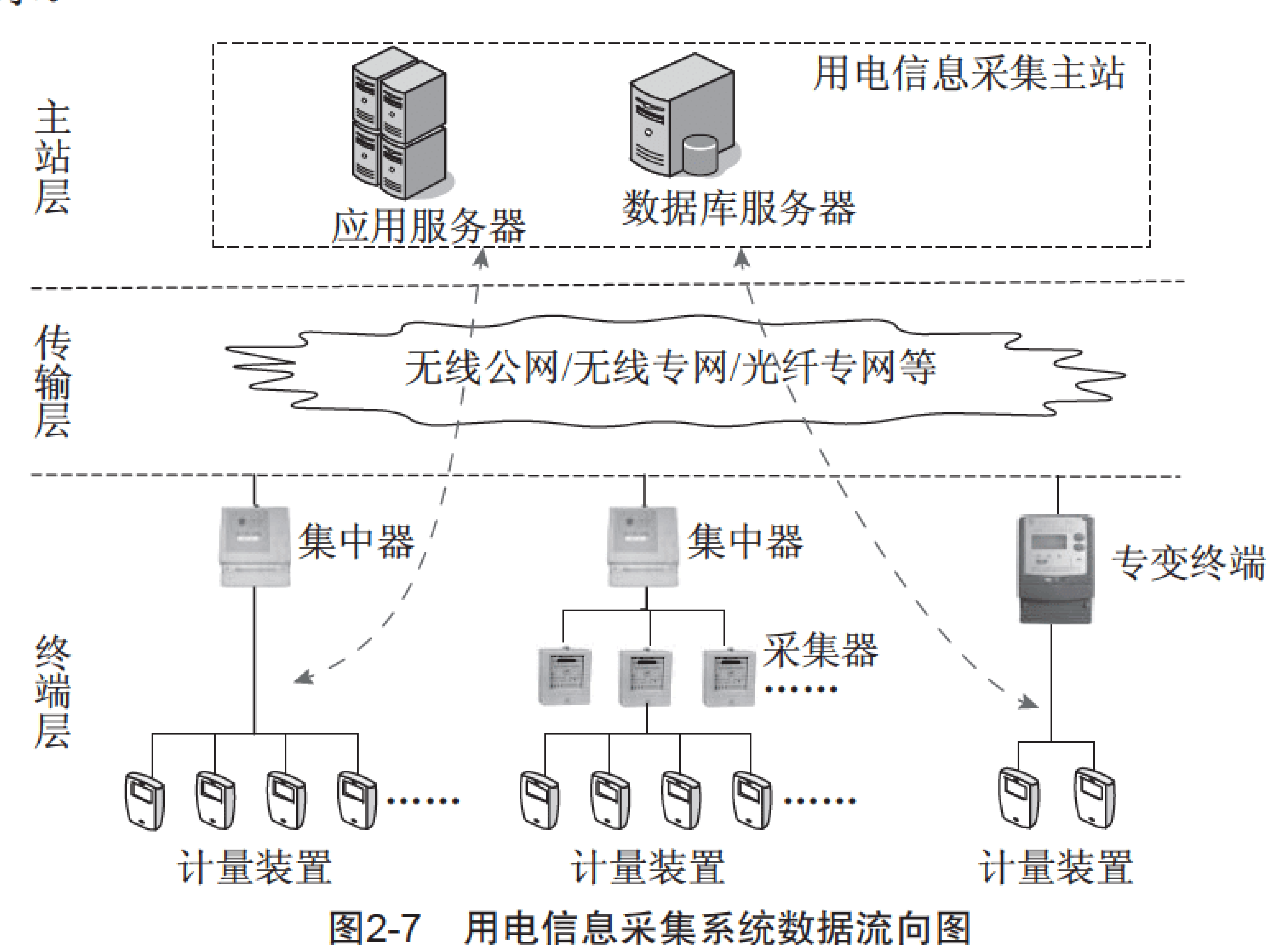


图2-7 用电信息采集系统数据流向图

（2）带宽及采集间隔

用电信息采集业务采集的数据项主要包括电能表数据采集、状态量采集、交流模拟量采集、直流模拟量采集等。

（3）传输距离

用电信息采集终端至主站包含两部分，终端至变电站和变电站至主站的距离。若采用有线通信方式，则根据台区面积和位置而变化，一般在20km范围内。

（4）实时性

电信息采集系统的实时性要求包括：主站巡检终端重要信息（重要状态信息及总加功率和电能量）时间＜15min；系统控制操作响应时间（遥控命令下达至终端响应的时间）≤5s；常规数据召测和设置响应时间（指主站发送召测命令到主站显示数据的时间）＜15s；历史数据召测响应时间（指主站发送召测命令到主站显示数据的时间）＜30s；系

统对客户侧事件的响应时间≤30min。

（5）可靠性

用电信息采集的可靠性包括：遥控正确率≥99.99%；一次采集成功率≥95%；周期采集成功率≥99.5%（非设备故障和非通信故障条件下）。

（6）其他要求

用电信息采集终端部署于室外，多部署于楼道、屋檐等易于接入计量装置的地点，一般情况下不可移动。为了后期运行维护需要，内置通信模块均要求可管可控，方便管理者进行远程通信配置，判断故障点位置。对于专变采集终端，在非通信状态下，采用单相供电的终端，有功功耗应不大于7W，视在功耗应不大于15VA；采用三相供电的终端，每相有功功耗应不大于5W，视在功耗不大于10VA；电流输入回路功率消耗不大于0.25VA（单相）；电压输入回路功率消耗不大于0.5VA（单相）。对于集中抄表终端，在非通信状态下，采集器消耗的视在功率应不大于5VA、有功功率应不大于3W；集中器消耗的视在功率应不大于15VA、有功功率应不大于10W。

2. 电动汽车充电站（桩）

1）业务概况

车联网平台业务系统架构主要包括平台层、网络层、终端层。平台层主要指车联网平台系统，充电终端设施主要包括集中充电站及充电桩，充电桩内置充电桩通信终端，终端将采集的数据通过VPN专线传输至平台主站，如图2-8所示。

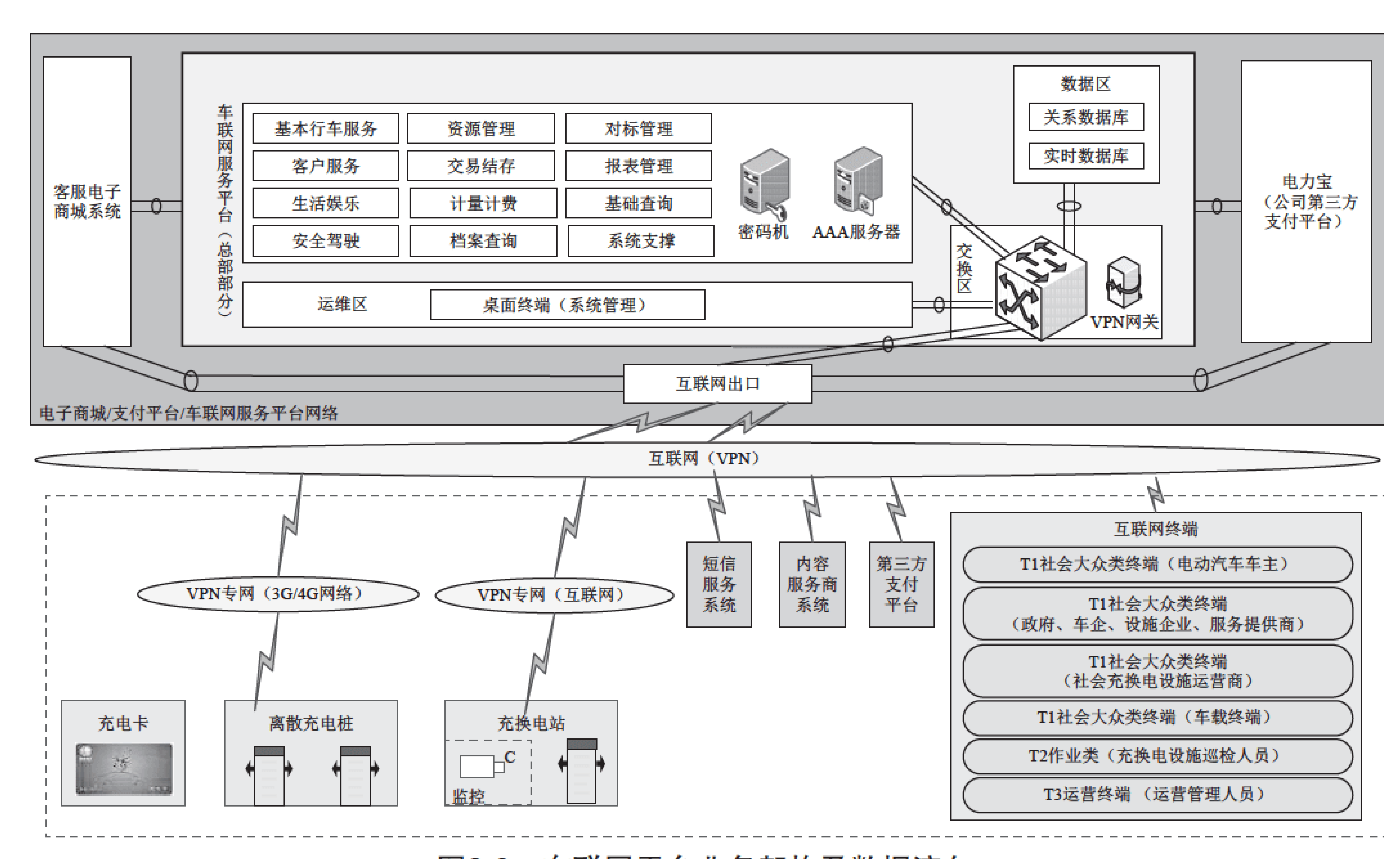


图2-8　车联网平台业务架构及数据流向

充电桩采用计量数据为营销用电信息采集业务系统范畴，不包含在车联网平台内，充

电桩用电信息采集业务按照现有用电信息采集系统所采用的无线公网通道进行建设。对于集中式充电站，一般情况下用电信息采集系统仅采集关口表电能信息。充电设备状态、计费等信息通过互联网上传至车联网平台。现阶段车联网平台采集公司范围内充电桩用电计量信息与各省电力公司单独结算。电动汽车充电站（桩）数据流向如图2-9所示。

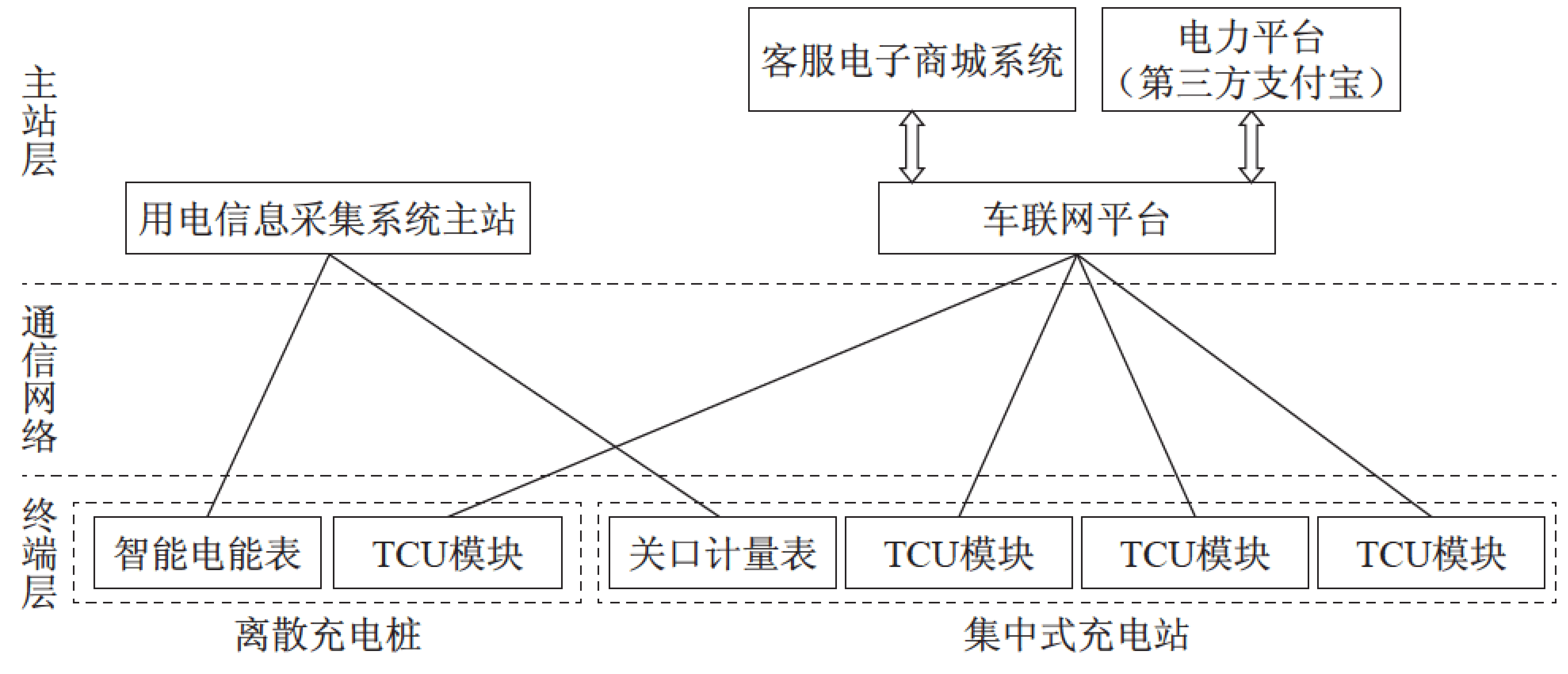


图2-9　电动汽车充电站（桩）数据流向

2）通信需求

（1）数据类型及数据流向

充电桩与车联网平台之间双向点对点通信，主站下发召测、计费等命令，终端上传设备、计量等信息。充电站由数十至数百个充电桩组成，每个充电桩与车联网平台之间通信，充电桩之间无信息传输需求。集中式充电站具备视频监控业务，采用本地存储方式，现阶段无须上传后台系统。

（2）带宽及采集间隔

由数据采集表计算可知：单个充电桩数据总量=267×8/1024=2kbps，考虑给予一定通信信道预留，单个充电桩数据量按照4kbps进行计算。按照上述采集数据类型及数据量，则单个充电桩带宽要求为4kbps。电动汽车充电站（桩）数据流向如图2-10所示。

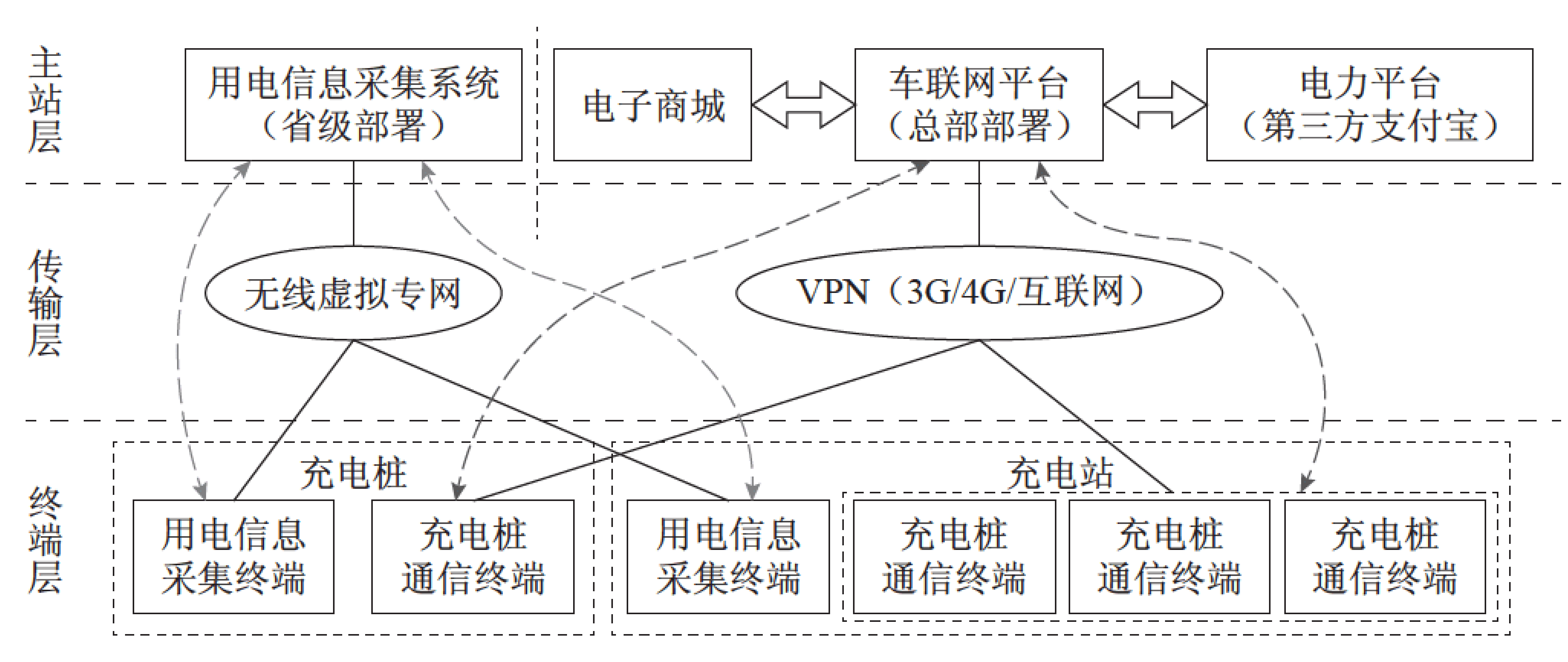


图2-10　电动汽车充电站（桩）数据流向

（3）传输距离

车联网平台系统为一级部署，充电桩和车联网平台主站直接通信。高速公路沿线充电站距离变电站一般在20km以上；城市核心区充电站距离变电站/开闭所约2～5km。充电桩分布广泛且分散，主要集中在居民区、企业、学校、商场等人流密集区域，距离变电站远近不一。

（4）可靠性

业务系统的可靠性要求为系统可靠性≥99.9%。

（5）实时性

业务系统的实时性要求，系统时延要求＜5s。

（6）信息安全要求

电动汽车充换电业务系统为信息安全等级保护3级，在主站边界需部署集成抗拒绝服务模块和防恶意代码攻击模块的防火墙、入侵检测系统和逻辑强隔离等安全措施，在终端应采用国家主管部门认可的密码算法保证通信过程中数据的保密性与完整性。

（7）其他要求

充电桩通信模块内置于充电桩内部的计费控制单元，充电桩自身对计费控制单元有一定的防水防尘措施，通信模块采用电信级即可。电动汽车充电需固定充电位置，不要求充电桩可移动，对移动性没有要求。通信模块内置于充电桩计费控制单元，要求通信模块功耗较低。为了后期运行维护需要，充电桩内置通信模块均要求可管可控，方便管理者进行远程通信配置，判断故障点位置。

2.2.3　用能服务业务

1. 智能家居

1）业务概况

在电力用户家庭内部部署智能交互终端、智能插座、智能家电等设备，实现对家用电器用电信息自动采集、发布、分析，开展烟雾探测、燃气泄漏探测、家庭安防、紧急求助、三表抄收等增值业务；通过智能交互终端与小区低压电力通信网互联，利用95598互动网站和智能家居服务平台，实现智能家居远程控制与管理。智能家居逻辑结构如图2-11所示。

智能家居逻辑上分为设备层、通信层和主站层。设备层包括智能家庭网关、智能交互终端等相关设备，通信层实现设备之间、设备与主站的信息传输，主站层包括智能小区主站智能家居模块和95598互动服务网站。其中，智能小区建设内容涵盖设备层、通信层和智能小区主站智能家居模块。

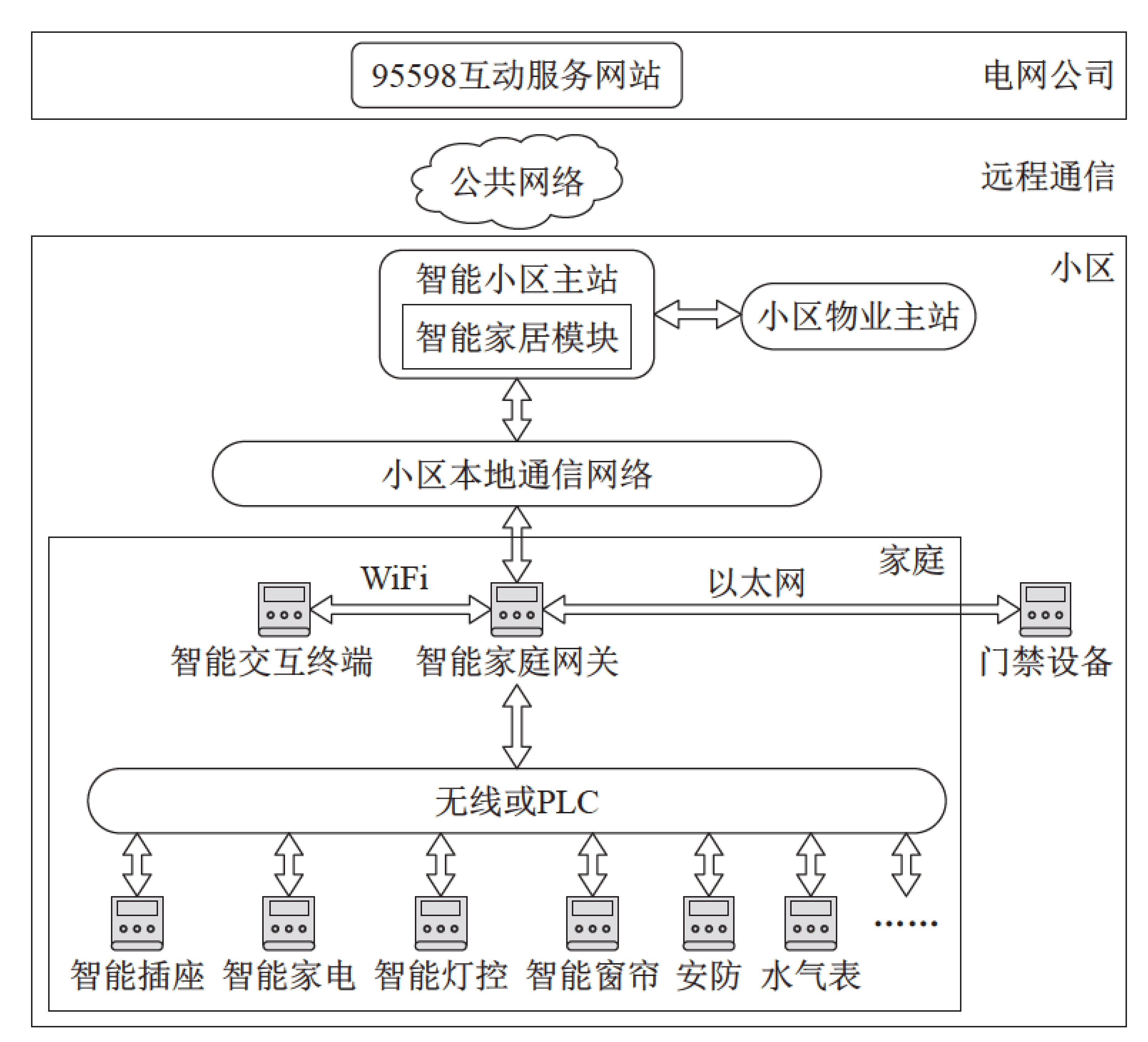


图2-11　智能家居逻辑结构

2）通信需求

智能小区主站（含智能家居模块）控制操作命令响应时间（控制命令下达至终端响应的时间≤5s，控制正确率≥99.99%。

智能家居业务用于传输家电、语音、家庭安防等信息，传输速率约为1～4Mbps，传输时延为百毫秒级。

智能小区通信网络的技术要求如下：

① 小区通信网络带宽的配置应充分考虑当前及未来智能小区各项业务需求。若支撑“三网融合”、智能家居业务，每户带宽应大于30Mbps；若仅支撑用电信息采集、小区配电自动化等业务，带宽应不小于500bps。

② 小区通信网络采用光纤通信时，传输误码率不大于10^{-10}；采用230MHz无线通信时，传输误码率不大于10^{-5}；采用PLC通信时，传输误码率不大于10^{-5}；采用RS-485通信时，传输误码率不大于10^{-9}。

③ 小区通信网络设备的性能及组网应符合DL/T 395—2010、Q/GDW 521—2010、Q/GDW 541—2010等标准的规定。

④ 小区通信网络建设应符合GB/T 22240—2008、Q/GDW 594—2011、Q/GDW 595—2011等信息安全相关标准和规定，实现小区电力专网和小区公共网络的物理隔离和纵向安全防护。

⑤ 智能小区业务进行信息交互，所用信息通信网不能与调度数据网相链接。

2. 智能营业厅

1）业务概况

智能营业厅利用信息化手段，实现交互式、人性化、自助式的供电服务，包含实体营业厅、互动终端营业厅、网上营业厅、手机营业厅、短信营业厅、呼叫中心营业厅、车载移动营业厅、用电自助终端等多种实现形式。营业厅需与营业厅服务管理系统、营销业务应用系统和其他相关业务系统、95598供电服务平台及银行系统实现数据交互。智能营业厅架构如图2-12所示。

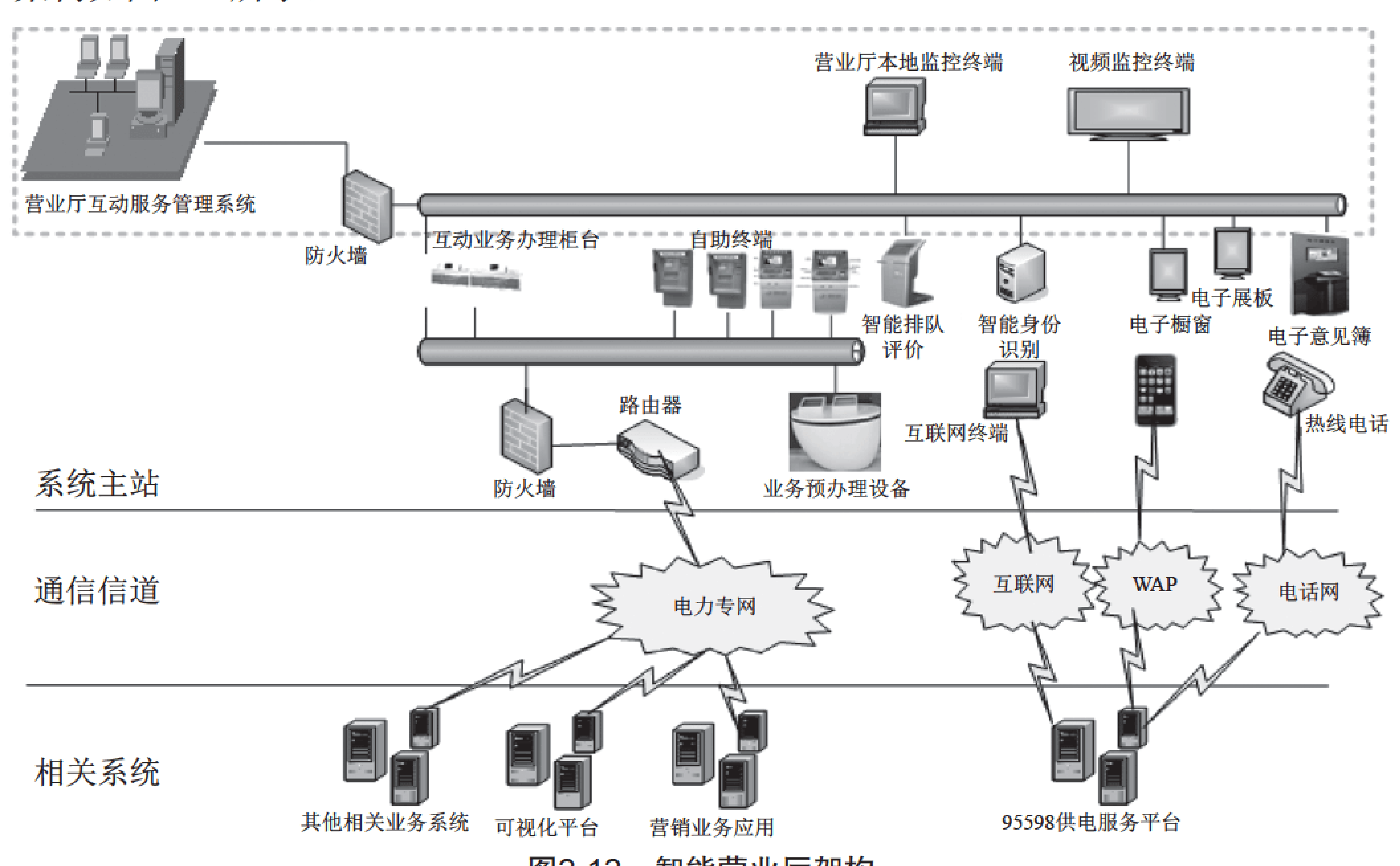


图2-12　智能营业厅架构

2）通信需求

不同类型供电营业厅的生产管理、经营服务等典型业务配置需求如表2-3所示。

表2-3　供电营业厅典型业务配置需求

类型	业务类型						
	营销系统	ERP	OA	网络培训	视频会议系统	行政电话	视频监控
A级	√	√	√	√	√	√	√
B级	√	√	√	○	√	√	√
C级	√	√	√	○	√	√	√
D级	√	-	-	-	-	-	○

注：①“√”表示包括此项内容；“○”表示此项内容可选；“-”表示无此项内容或不做要求。
②上述业务配置为典型推荐值，各单位可根据实际需求进行适当调整。
③上述各类业务应优先通过数据通信网承载。

假定营业厅有6台业务终端，4个视频监控点进行估算，则含视频带宽总需求约为6.9Mbps，如表2-4所示。

表2-4　营业厅出口业务流量　　单位：Mbps

序　号	业务组成	业务流量	链路数量	并发比例	小　计
1	营销系统	0.06	6	50%	0.18
2	OA	0.06	6	50%	0.18
3	网络培训	2	1	100%	2
4	软视频会议系统	2	1	100%	2
5	行政电话	0.5	1	100%	0.5
6	视频监控	2	4	25%	2
7	业务净流量总计				6.86

接入网实现实体营业厅、互动终端营业厅的视频监控、柜台终端和自助服务终端、独立布置的自助终端和车载移动营业厅的通信接入，承载用户档案、用电信息、变更业务、缴费业务及服务管理等数据和视频业务，视频监控带宽要求最高。实体营业厅、互动终端营业厅优先使用光纤专网接入，独立布置的自助终端优先通过光纤或无线专网接入，车载移动营业厅通过无线专网接入，手机营业厅、短信营业厅、网上营业厅可以通过电力专用VPN网络专线接入。

2.2.4　移动互联业务

1. 移动巡检

1）业务概况

在“营配调一体化”背景下，移动巡检包括配电工区的移动巡视、移动检修等业务。

移动巡视业务包括现场巡视作业、巡视签到和巡视监控等功能。巡视作业为运维检修人员在规定时间、规定地点对配电工区线路、管道、设备等进行巡视检查，通过PDA设备生成文字或图片形式的巡检记录，储存在本地，巡检结束后上传PMS。巡视签到指巡检人员巡检时通过手持移动端扫描设备上的二维码完成巡检设备签到，保证了所有任务中要巡检的设备都能被检查，不会出现漏检的情况。巡视监控指巡检中心根据实际需求准确监视巡检人员工作状况，可实现对巡检人员的定位及巡检轨迹回放等功能。

移动检修业务包括巡检管理、现场巡检人员管控、远程协助和移动办公等几个方面的功能。巡检管理指管理人员根据巡检设备或巡检点的要求设置不同的检查项目，自动或手动生成巡检任务，并将任务派发给现场巡检人员，综合实现任务制订、任务审批、任务下达、任务跟踪等一系列功能。现场巡检人员管控主要实现巡检员、缺陷、安全隐患、设备等位置和分布在地图上的显示等功能。远程协助指检修人员通过文字、图片或语音形式，将线路、管道、设备故障情况实时上传巡检中心或专家系统，请求远程协助。专家系统将维修方案实时下发移动巡检终端，现场检修人员可依据专家意见按步骤进行维修。移动办公包括待办事宜、待阅事宜、电子邮件、移动审批、移动信息录入、巡检信息查询、组织

机构管理、日程管理、联系人管理、公文浏览、下载和转发、系统管理等常用的功能。

2）通信需求

移动巡检业务包括移动巡视和移动检修两大类业务。移动巡视业务如不需要巡视监控功能，则其余功能均可本地实现，不需要远程通信。移动检修业务，因具有远程协助、移动办公等高级功能，需要实现巡检终端与巡检中心之间的通信，传输的数据包括文字、图片、视频等多种形式。以典型业务类型分析，不同业务传输速率范围不同：语音业务为8～64kbps；视频业务为384kbps～2Mbps；数据业务为64kbps～2Mbps。其中，语音和视频类业务对时延和可靠性要求较高。

当前，移动巡检业务并没有形成国网或省级统一部署，只是在部分地市公司开展了试点应用，所采用的通信方式主要包括无线专网（4G）和无线公网（3G/4G）。

2. 无人机巡检业务

1）业务概况

无人机巡线技术主要被应用于电力线与杆塔巡线、输电线路巡检、线路施工测绘等，通过地面控制站进行操控拍摄，完成图像的实时回传与快速拼接，实现复杂地形、恶劣环境下的现场信息获取。

无人机巡检系统是利用无人机搭载可见光、红外等检测设备，完成架空输电线路巡检任务的作业系统。一般由无人机分系统、任务载荷分系统和综合保障分系统组成，包括无人直升机（按结构形式一般分为单旋翼带尾桨式和多旋翼式）巡检系统和固定翼无人机巡检系统。

线路本体巡检、故障巡检和其他精细化巡检宜优先配置无人直升机巡检系统；线路通道巡检、灾情普查和其他快速普查宜优先配置固定翼无人机巡检系统。

2）通信需求

无人机应配置插拔式存储设备，存储空间应能满足无人机巡检系统最大巡检能力的要求，固定翼无人机巡检系统不小于64GB，小型无人直升机巡检系统不小于32GB，中型无人直升机巡检系统不小于64GB。无人机应配置可见光摄像机和无线图像传输系统，图像清晰度应能满足巡检要求（标清及以上），传输延时不宜超过300ms。

固定翼无人机巡检系统满足以下通信要求：

① 传输带宽≥2M（标清），图传时延≤300ms。

② 数传延时≤80ms。

③ 通视条件下，最小数传距离≥20km。

④ 通视条件下，最小图传距离≥10km。

固定翼无人机巡检航速度宜在60～120km/h 范围内。

无人直升机巡检系统通信功能应满足：

① 实现无人直升机分系统测控数据的上传和下传。

② 实现任务载荷分系统测控数据的上传和下传。

③ 在通信链路不中断的情况下具有实时视频传输功能。

中型无人直升机通信性能应满足：

① 数传延时≤80ms，误码率≤1×10^{-6}。

② 传输带宽≥2M，图传时延≤300ms。

③ 距地面高度60m时最小数传通信距离≥5km。

④ 距地面高度60m时最小图传通信距离≥5km。

小型无人直升机通信性能应满足：

① 数传延时≤20ms，误码率≤1×10^{-6}。

② 传输带宽≥2M（标清），图传时延≤300ms。

③ 距地面高度40m时数传距离不小于2km。

④ 距地面高度40m时图传距离不小于2km。

根据工信部无线电频率划分规定，无人机通信频段限制为840.5～845MHz、1430～1444MHz、2408～2440MHz三个频段。840.5～845MHz可用于无人机上行遥控链路，其中841～845MHz也可采用时分方式用于上行遥控和下行遥测。1430～1444MHz可用于无人机下行遥测和信息传输链路，其中1430～1438MHz主要用于警用无人机控制及视频传输，其他无人机使用1438～1444MHz频段。2408～2440MHz可用于无人机上行遥控、下行遥测及信息传输链路的备份频段。

无人机通信系统主要实现无人机遥控信号、巡检图像与遥控操作台的信息传输。遥控操作速率100kbps以内，实时性、可靠性要求较高。巡检图像传输速率2Mbps以上，实时性、可靠性要求较高，传输距离较远。

3. 机器人巡检

1）业务概况

巡检系统主要由巡检机器人、监控后台、电源系统等组成，是能够自主进行变电站巡检作业或远程视频巡视的变电站巡检系统。

巡检机器人是通过机器人搭载的可见光摄影机、红外热成像仪和局放综合检测设备，对设备进行观测，实现对设备缺陷的智能诊断和综合管理，自动生成线路及设备健康状态检测报告，并将检测数据和诊断结果自动上传至PMS系统，为配电网状态管控提供基础数据。智能巡检机器人主要由控制系统、驱动系统、DGPS定位系统组成。

运动控制系统：实现机器人动力驱动，根据系统路径规划和遥控指令实现车体的运动控制，包括速度、位置、加速度控制等。根据上层控制指令的不同，设计的运动控制系统的实现包括自主行驶和遥控行驶两种形式。

DGPS定位系统（Differential Global Positioning System）：称为差分全球定位系统，是一个中距离圆形轨道卫星定位系统。它可以为地球表面绝大部分地区提供准确的定位和高

精度的时间基准。巡检机器人可以通过DGPS定位进行路径选择，也可通过视频遥控控制行走的路径。

图2-13所示为机器人巡检系统结构示意图。

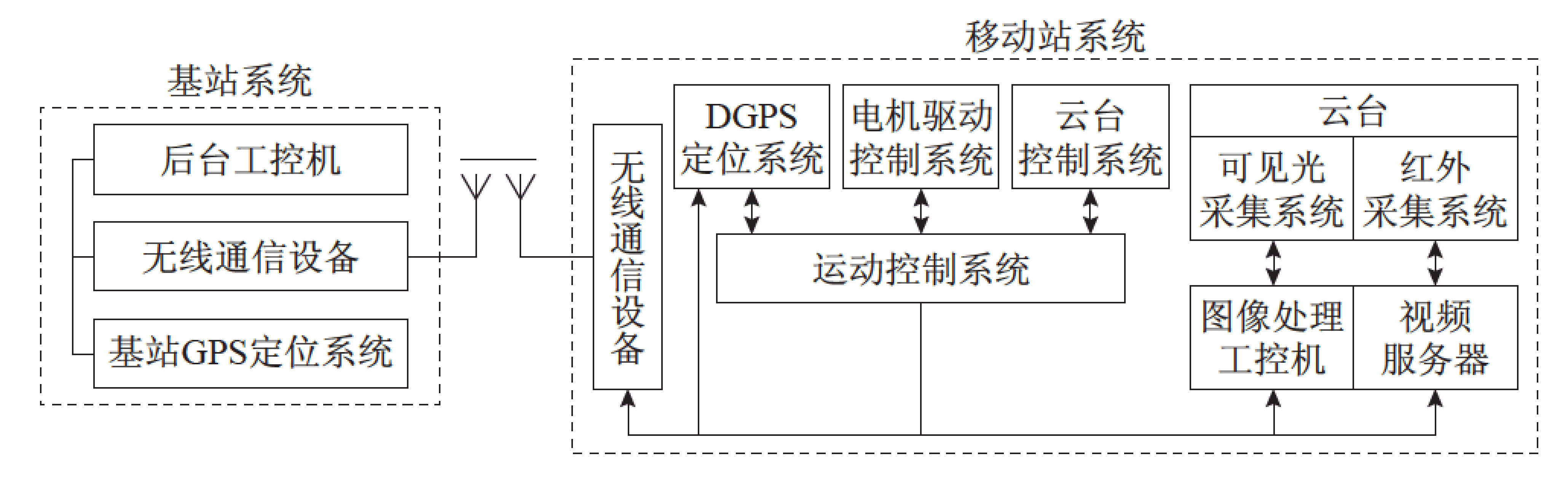


图2-13　机器人巡检系统结构示意图

2）通信需求

监控后台通信需求：

具备对巡检系统巡检参数和检测设备工作状态参数的遥测功能，距离不小于1km。

可见光视频可实现全向、实时传输，传输距离不小于1km。

红外影像可实现全向、实时传输，传输距离不小于1km。

系统宜具备对时功能，可采用网络对时、SNTP或GPS、北斗对时等方式，对时周期和精度应符合工程实际的需求。

远程集控系统通信需求：

远程集控后台应能与本地监控后台进行双向信息交互，信息交互内容包括检测数据和机器人本体状态数据。

数传误码率≤10^{-6}，时延≤20ms。

图传时延≤300ms。

数据类型包括图像、设备诊断等信息，数据传输速率要求大于2Mbps，对通信时延、可靠性要求较高。变电站内巡检一般选择WiFi技术组网。在无线专网覆盖区域，可选用无线专网进行承载；其次为4G无线公网。

4. 基建现场视频监控

1）业务概况

视频监控系统能够把施工现场画面通过网络技术传到办公管理区域，施工管理人员可以通过实时监控信息对现场施工进行了解和掌握，然后根据施工进度和施工质量对施工过程进行有效控制和管理，保障了基建施工的质量、安全与周期。

2）通信需求

电力基建现场一般部署1至3台视频监控终端，每路普清视频的传输速率要求大于2Mbps，每路高清视频的传输速率要求大于4Mbps，下行云台控制信息的传输速率一般小

于10kbps。由于施工现场视频监控系统为临时性部署，对实时性、可靠性安全要求较低，在光纤专网与无线专网覆盖区域，优先选用光纤专网或无线专网进行业务承载，其次可选择在现场部署无线专网基站，通过连接光纤网络传输至后台主站，最后可选用3G/4G无线公网承载（考虑经济成本，仅传输图片）。

2.3 多业务公共接入分析

当前终端通信接入网采用随业务系统建设的模式，以致现有终端通信接入网由多个相互独立的通信网络组成，通信网络与接入业务耦合关联性较强，终端通信接入网呈现出多种通信网络并存、每种通信网络资源利用率不高、网络重复建设的现象。这种建设模式在智能电网发展前期能够很好地适应配用电业务接入需求，主要表现在各种业务之间可实现物理隔离、专网专用，满足不同业务部门的安全接入需求；通信网为业务系统量身定制，能很好地满足业务需求。由于早期智能配用电系统业务种类少、网络建设规模小，即使为每个业务单独建设网络也不至于造成通信资源的浪费。

随着终端通信接入网规模逐渐增大，这种随业务系统单独建设通信网络的建设模式逐渐暴露出问题，具体包括：不同业务的接入网自成体系，资源无法共享，单一网络资源利用率不高，通信网兼容性和扩展性不足，重复建设严重，通信网络建设费用显著增多；接入网形成多张独立网络，网络结构复杂，难以实现统一标准、统一规划、统一建设，不满足公司集约化建设要求；通信网运维人员分散于各个业务部门，运维工作管理困难，通信网整体可靠性有待完善。因此，建设终端通信接入网公共平台，统一调度通信网资源，对接入网通信线路和设备等资源高效复用，实现各种业务的统一接入需求十分迫切。

2.4 总　　结

本章主要进行了终端通信接入网的多业务应用场景与应用的需求分析，包括配电环节业务、用电环节业务、用电服务业务和移动互联业务。每种业务分别从业务概况和通信需求两个方面进行了详细说明。最后又进行了多业务公共接入分析，得出了实现各种业务的统一接入需求十分迫切的结论。

第3章
业务与接入网技术匹配性分析



3.1 终端通信接入网技术体系

终端通信接入网（以下简称“接入网”）是电力系统骨干通信网络的延伸，是电力通信网的重要组成部分，由业务节点接口（SNI）和用户网络接口（UNI）之间一系列传送实体（如线路设施和传输设施等）组成，提供配电与用电业务终端同电力骨干通信网络的连接，实现配用电业务终端与系统间的信息交互，具有业务承载和信息传送功能，分为10kV通信接入网和0.4kV通信接入网两部分。

10kV通信接入网的范围为变电站10kV出线至开关站（开闭所）、充电站、环网单元（柜）、柱上开关、电缆分支箱、（配电室、柱上、箱式）10kV变压器等（以下简称配电站点）。0.4kV通信接入网的范围为变压器0.4kV出线至用户表计、充电桩、营业网点、电力光纤到户室内终端等，支撑用户用电信息采集系统本地通信（用户表计至采集器、集中器）、用电营业服务、用户双向互动等通信接入业务。10kV通信接入网承载配电自动化接入层通信、用电信息采集远程通信、电动汽车充电站（桩）通信、分布式电源接入通信等业务；0.4kV通信接入网承载用电信息采集本地通信、光纤到户等业务。

1. 接入网技术体系现状

终端通信接入网承载配电自动化、用电信息采集、分布式电源、电动汽车充电站、营业场所接入等业务，主要采用配电自动化通信技术、用电信息采集通信技术、分布式电源通信接入技术以及电动汽车充电站（桩）通信系统。10kV通信接入网光缆总长度达到14.94万km，新建及改造光缆8.6万km。

配电自动化系统当前应用的通信技术主要包括光纤、电力线载波、无线公网和无线专网等，实现了业务终端通信全覆盖，其中光纤覆盖占比16.6%、无线公网占比82%、载波通信占比1%、无线专网占比0.4%。配电网自动化系统主站与子站及终端的通信方式原则上以电力光纤通信为主，并优先采用，主站与主干配电网开闭所的通信应当采用电力光纤；当采用EPON、GPON或光以太网络等技术时应使用独立纤芯或波长，配网监控专用通信网络应能与调度数据网络相连。对于不具备电力光纤通信条件的末梢配电终端和只采集遥信、遥测的配电终端，可采用无线公网（TD-SCDMA、GPRS、CDMA、230MHz

等，优先选择TD-SCDMA）方式进行通信。配电自动化终端可通过EPON、无线专网、无线公网等多种模式与配电主站进行通信。

用电信息采集的通信终端多以模块的形式嵌入在业务终端中，业务终端具备通信功能的数量即为相应的通信模块数量。

用电信息采集远程通信网络完成主站系统和现场通信终端之间的数据传输通信功能，通信方式主要有无线公网、光纤专网、230MHz无线专网、电话PSTN等，主站系统可以同时支持各种通信信道类型，其中无线公网覆盖占比98.32%、其他通信技术占比1.68%。

本地信道用于现场终端到表计的通信连接，通信技术包括电力线载波、RS-485总线、微功率无线等。高压用户在配电间安装专变采集终端到就近的计量表计，采用RS-485总线方式连接，低压用户一般选取低压电力线载波、微功率无线、RS-485总线等通信方式灵活组网方案。其中载波覆盖占比69.5%、RS-485覆盖占比25.6%、微功率无线占比4.5%，其他占比0.4%。受台区面积、传输距离、采集周期、环境干扰等因素制约，本地通信一次成功率相对较低。

目前，35/10kV分布式电源一体化装置主要依靠光纤通信技术传输数据，并网点至变电站通信采用EPON/工业以太网方式，再通过地市级骨干通信网上传到监控系统主站。关口计量信息由用电信息采集系统分布式电源监控终端采集并直接与用电信息采集系统交互信息，采用无线公网通信。380/220V分布式电源只有关口计量信息，分布式电源监控终端与用电信息采集系统实现信息交互采用无线公网通信方式。

并网投产的10kV分布式电源站点已实现通信全覆盖，光纤覆盖占比89%，中压电力线载波占比5%，无线公网占比5%，无线专网占比1%。380/220V分布式电源并网接入通信以无线公网方式为主。35/10kV分布式电源含有控制类信息，目前主要依靠光纤通信承载。380/220V分布式电源采用租用无线公网方式实现数据传输。

电动汽车充电站（桩）采用车联网平台的模式进行建设，通信方式采用无线虚拟专网实现站（桩）至平台间的互联互通。目前电动汽车充电站光纤覆盖占比92%，无线公网覆盖占比8%；电动汽车充电桩无线公网占比85.4%，光纤占比14.6%。

分散充电桩内置联通、移动各1张SIM卡，为主备关系，根据信号强弱程度进行切换，通过无线公网直接传输至上海灾备中心，完成终端至主站间的通信。充电桩用采计量数据为营销用电信息采集业务系统范畴，不包含在车联网平台内，充电桩用电信息采集业务按照现有用电信息采集系统所采用的无线公网通道进行建设。对于集中式充电站，用电信息采集系统仅采集关口表电能信息，充电站内充电桩设备状态、计费等信息暂时仍以充电桩为单位通过无线公网上传至车联网平台。

2. 存在的问题

通过对接入网建设现状的分析表明，接入网建设主要存在以下问题：

① 组网模式方面，通信网络建设分散，接入网与业务系统“紧耦合”，网络建设分

散且重复，通信资源利用率低，存在多张接入网并存的问题。

② 技术选型方面，通信部门参与业务系统（通信部分）的建设深度不够，缺乏业务与通信技术的匹配分析，导致现阶段的接入网技术政策（特别是无线通信技术）不够科学、完备，难以为新能源接入、电动汽车等新增业务提供快速、灵活、高效技术支撑。

③ 存在配网光纤建设成本过高，无线专网频率资源不足，无线公网通道的质量难以保障，配电自动化难以兼顾用采系统远程通信，10kV接入网与0.4kV接入网上下衔接渠道尚未打通等问题。

3.2 终端通信接入网技术应用方式分析

3.2.1 匹配分析概述

配用电业务与通信技术匹配的分析图如图3-1所示。

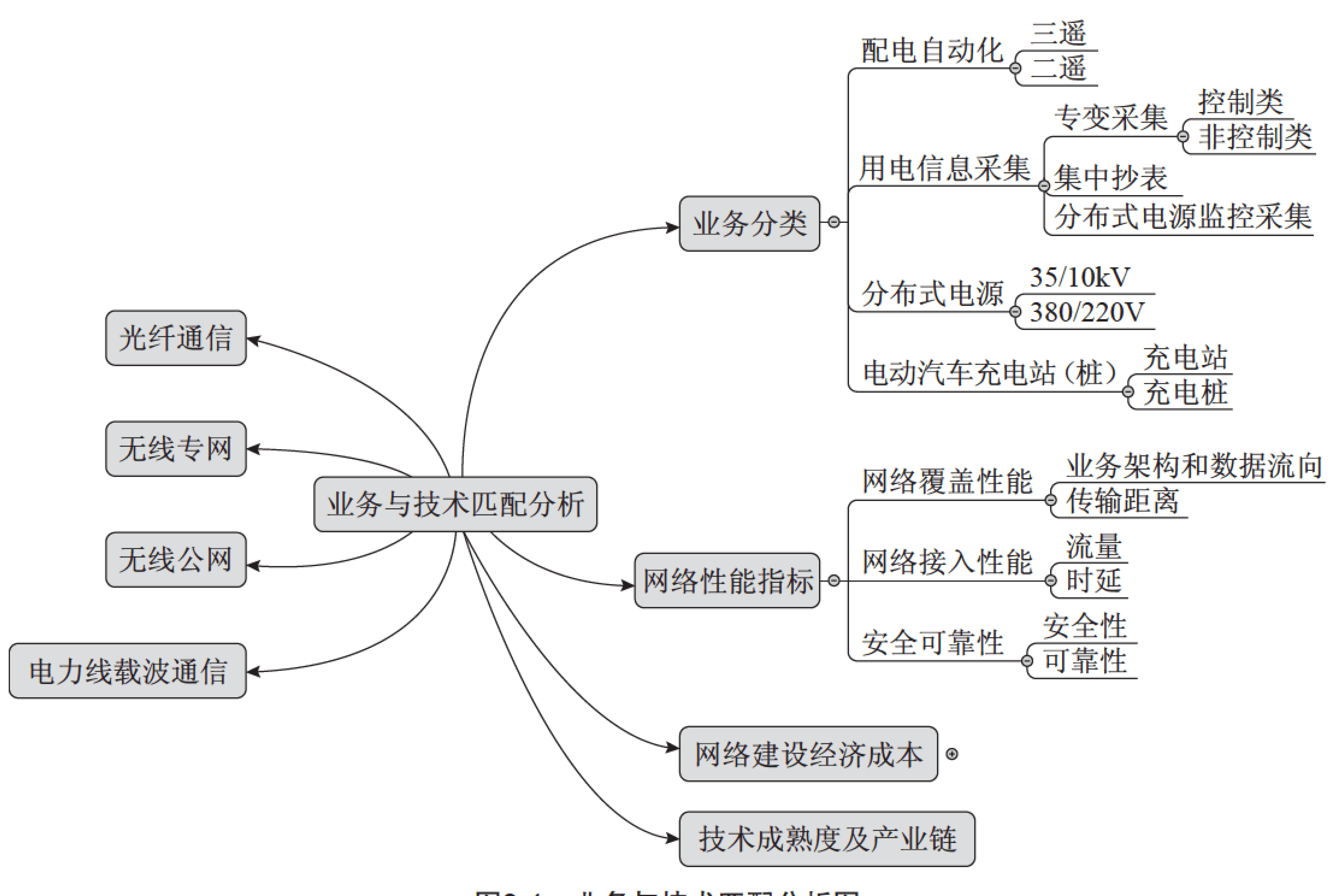


图3-1 业务与技术匹配分析图

通过业务分类、网络性能指标、网络建设经济成本、技术成熟度及产业链四个维度对光纤通信、无线专网、无线公网、电力线载波通信进行匹配分析，为接入网通信系统设计

提供依据。网络性能指标包括网络覆盖、带宽、时延、安全性、可靠性等。

3.2.2　匹配原则

配电自动化业务与技术匹配遵循系统性、客观性、可比性、实用性原则。

系统性原则：以各业务中的不同类型报文为目标，要反映所有因素对最终决策目标的整体影响，重视决策问题各维度因素的层次性和相关性，反映出不同业务体系下对于技术选型的内部关联。

客观性原则：决策指标的筛选、归类、分析和评价应采取科学化、程序化方法，指标体系中应根据各决策指标的迫切程度客观确定各指标权重，并综合考虑、采纳领域专家评价建议，尽量避免主观随意性。

可比性原则：各子目标的分解和设计既要注意业务系统的性质对于通信各方性能要求的横向比较，又要注意各通信技术在纵向上对应各要求的匹配程度。

实用性原则：各决策指标设计要含义明确、计算简便。

1. 匹配步骤

具体匹配步骤如下。

步骤1　分析业务，提出业务各类指标要求。业务指标要求包括组网架构、带宽、传输距离、实时性、可靠性、成本、技术成熟度及产业链、安全性共7个指标。

步骤2　从业务指标要求方面分析接入网通信技术指标。

步骤3　对业务的单个业务指标进行通信技术匹配排序，采用线性比例变化法以匹配度最高的技术为基准1，按照排序顺序均分递减确定每种技术的匹配度参数。

步骤4　根据业务类型，确定价值因数。价值因数无法用科学手段进行检测或处理时，需要决策者进行价值判断。每种业务类型的价值因数根据经验值评估确定。

步骤5　根据步骤3和步骤4的结果，计算得出每种技术的综合匹配值，再根据综合匹配值排序。

步骤6　根据技术综合匹配值排序，结合业务分布特点等实际情况，得出每种业务类型的技术政策。

2. 匹配计算方法

从组网架构、带宽、传输距离、实时性、可靠性、成本、技术成熟度及产业链、安全性等方面开展匹配。根据匹配原则，确立以下匹配模型。

X_i=属性集{组网结构、带宽、传输距离、实时性、可靠性、成本、技术成熟度及产业链、安全性}，i=1，2，…，n，S_{ij}为X_i方面第j种技术的匹配度参数，匹配度参数采用归一化算法，以排名第一的技术为基准数1，其他技术采用线性比例变化法，按照排序均

分递减。

$Y(y_i)$=价值因素，价值因素无法用科学手段进行检测或处理，需要决策者进行价值判断。y_i根据业务不同，采用经验法判断得出。

综合匹配值集合$Z(z_i)=\{z_1, z_2, z_3, z_4, \cdots, z_8\}$，其中$z_1$为EPON匹配值，$z_2$为工业以太网匹配值、$z_3$为中压PLC匹配值，依此类推，$z_8$为无线公网4G匹配值。$Z_i=\sum S_{ij} \cdot y_i$，其中$i=1, 2, \cdots, 8$；$j=1, 2, \cdots, 8$。

3.2.3 配电自动化

1. 业务与通信技术匹配

1）组网结构及数据流向

配电自动化系统以地市为单位部署，主站位于地市调度中心，配电终端沿配电线路部署，终端与主站之间点对点双向通信。

中压PLC为电力特有通信技术，利用配电线路传输数据，网络拓扑与电网架构完全吻合；光纤专网借助随配电线路敷设的光缆传输数据，网络拓扑与电网架构基本吻合；无线专网为电力自建网络，专网专用，核心网部署在地市，基站部署在变电站等电力场所，业务数据在基站实现汇聚，网络拓扑与电网架构大致吻合；无线公网为租用网络，数据通过公网专线在地市汇聚，网络拓扑与电网架构无关。基于以上分析，业务架构与数据流向匹配度由高到低排序表如表3-1所示。

表3-1　业务架构匹配度排序表

通信技术	中压PLC	光纤专网	无线专网	无线公网	备注
业务架构要求	电力特有，数据利用配电线路传输	光纤随配电线路敷设	根据需求自建基站，数据直接在变电站汇聚	租用网络，运营商汇聚数据，在省/市专线接入	与电网架构吻合
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

中压PLC、光纤专网、无线专网匹配度较高，无线公网匹配度较低。

2）带宽及采集间隔

目前，配电自动化主站对终端的常规召测频率根据需要设置为1～60min一次，没有统一规定；终端网络连接心跳数据帧为30s一次；遥信、遥控方面，主站下发命令或终端设备因突发事件主动上传数据时，采集间隔不固定。遥测方面，采用光纤通信的配电终端一般设置为电压变化1V，电流变化10mA往主站上送一次数据；采用无线通信方式时，配电

终端一般设置为电压波动1V，电流波动50mA往主站上送一次数据。

按配电自动化单个终端的实时数据传输速率10.2kbps进行匹配，各类通信技术速率指标如下：2G无线公网传输速率为10～90kbps，中压PLC传输速率为10～100kbps，3G无线公网传输速率为30～700kbps，TD-LTE 230MHz无线专网传输速率为500kbps～1Mbps，TD-LTE 1800MHz无线专网传输速率为5～10Mbps，4G无线公网传输速率为5～10Mbps，工业以太网传输速率大于5/50Mbps（100/1000Mbps带宽，按20个终端计算），EPON传输速率大于30Mbps（1.25Gbps共享，按32个终端计算）；通信技术最小速率与业务匹配度排序如表3-2所示。

表3-2　带宽参数匹配度排序表

通信技术	2G	中压PLC	3G	TD-LTE 230MHz	TD-LTE 1800MHz	4G	工业以太网	EPON	备　注
速率值	10～90kbps	10～100kbps	30～700kbps	1M 带宽资源：500kbps～1Mbps	5M带宽资源：5～10Mbps	5～10Mbps	单终端≥5/50Mbps	单终端≥30Mbps	10.2kbps
排序结果	1	2	3	4	5	6	7	8	
匹配度参数	1	0.875	0.75	0.625	0.5	0.375	0.25	0.125	线性比例变化法：以最匹配为1，按照排序均分递减

无线公网2G、中压PLC匹配业务带宽要求，其他的通信技术可以提供更高带宽，但存在带宽资源浪费。无线公网的性能受运营商网络负荷影响，速率波动较大，中压载波在干扰较多、信道不稳定的情况下带宽较低。

3）传输距离

35/110kV变电站出线至用户的传输距离在20km范围内，EPON光纤通信技术传输距离小于20km，无线专网传输距离可根据需要进行区域覆盖，无线公网传输距离取决于运营商网络覆盖区域，工业以太网交换机技术传输距离大于20km，中压PLC技术传输距离为地埋小于2km、架空小于10km；各类通信技术传输距离与业务的匹配度由高到低排序如表3-3所示。

表3-3　传输距离匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　注
距离	＜20km	根据选用光模块不同传输距离不同，为1～80km	自建基站覆盖区域，可根据需要	运营商网络覆盖区域	不考虑中继，地埋＜2km、架空＜10km	＜20km
排序结果	1	2	3	4	5	

续表

通信技术	EPON	工业以太网	无 线 专 网	无 线 公 网	中压PLC	备　　注
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

EPON、无线专网、无线公网匹配业务带宽要求；工业以太网可覆盖更广区域；不考虑中继，中压PLC覆盖范围不满足要求。

4）实时性

配电自动化“三遥”业务时延要求≤6s（包括两次主站到终端命令传输时间，两次终端到主站命令传输时间）。“二遥”业务实时性要求相对较低，遥信时延要求为光纤通信方式＜2s，载波通信方式＜30s，无线通信方式＜60s；遥测时延要求为光纤通信方式＜2s，载波通信方式＜3s，无线通信方式＜30s。

EPON光纤通信技术传输时延为1.5ms，工业以太网交换机网络传输时延为10ms，无线专网传输时延为30～300ms，无线公网传输时延为600ms～2s，中压PLC传输时延为0.3s～3s。遥控业务实时性匹配度由高到低排序如表3-4所示。

表3-4　遥控业务实时性匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　　注
时延值	1.5ms	10ms	30～300ms	600ms～2s	0.3s～3s	＜1.5s
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

EPON、工业以太网、无线专网匹配遥控业务时延要求，其他通信技术不匹配。

“二遥”业务不同技术时延要求不同，不再进行排序对比。

遥信时延要求为光纤通信方式＜2s，载波通信方式＜30s，无线通信方式＜60s；遥测时延要求为光纤通信方式＜2s，载波通信方式＜3s，无线通信方式＜30s。因此各种通信技术均能满足要求。

5）可靠性

配电自动化对终端月在线率、遥控成功率、遥信动作正确率等要求较高，均在95%以上。

光纤专网依靠光纤传输，不受电磁干扰和雷电影响，EPON系统中光分路器为无源器件，设备使用寿命长，系统具备抗多点失效的能力，“手拉手”保护组网模式光纤保护倒换时间≤100ms；工业以太网交换机同样采用光纤线路，系统的无故障工作时间＞17520h，单台交换机的环网恢复时间不超过50ms。根据《电力用户用电信息采集系统设计导则：技术方案设计导则》（Q/GDW 378.3—2009）现场实测指标，光纤专网（EPON）数据采集一次成功率＞99%。

无线公网为租用网络，信道受天气、地形、网络负荷等因素影响、信号易受干扰，服务质量可变因素较多，尤其发生突发事件时，不能保证畅通，根据Q/GDW 378.3—2009规范中现场实测指标，无线公网（GPRS）数据采集一次成功率＞97%。无线专网为自建网络，专网专用，需要专业技术人员开展网络优化，在基站覆盖范围内，理论上可靠性高于无线公网，根据Q/GDW 378.3—2009规范中现场实测指标，无线专网（230数传电台）数据采集一次成功率＞97%。TD-LTE无线专网目前处于试点阶段，可靠性需进一步验证。中压载波易受电网环境干扰，信道稳定性较差，根据Q/GDW 378.3—2009规范中现场实测指标，中压PLC数据采集一次成功率＞85%，如表3-5所示。

表3-5　可靠性匹配度排序表

通信技术	光纤专网	无线专网	无线公网	中压PLC	备　注
可靠性	一次成功率＞99%（EPON）	一次成功率＞97%（230电台）	一次成功率＞97%（GPRS）	一次成功率＞85%	终端在线率、遥控成功率、遥信动作正确率等均大于95%
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

光纤专网、无线专网、无线公网匹配遥控业务可靠性要求，中压PLC不匹配。

6）技术成熟度及产业链的完整性

EPON具备完善的技术标准，技术成熟，产品成熟，产业链完整，已在公网大规模部署并运用于电力通信系统；工业以太网产品成熟，产业链完整，主要在数字化变电站中应用，但三层工业以太网交换机技术标准尚不完善，难以实现互联互通。

中压窄带电力线载波技术较为成熟，新型载波技术在研制试验，产业链完整。

无线公网为运营商无线网络，技术标准完备，技术成熟，产业链成熟完整。

TD-LTE 230MHz系统存在设备成本较高且近期内难以下降的问题。TD-LTE 1800MHz设备厂商较多，产业链较为完整。

各类通信技术的技术成熟度及产业链完整性排序如表3-6所示。

表3-6　各类通信技术成熟度及产业链排序表

通信技术	无线公网	EPON	工业以太网	中压PLC	TD-LTE 1800MHz	TD-LTE 230MHz
排序结果	1	2	3	4	5	6
参数值	1	0.83	0.67	0.5	0.33	0.17

7）安全性

通信技术安全性排序如表3-7所示。

表3-7　各类通信技术安全性匹配度排序表

排序结果	1	2	3	4
通信技术	光纤专网	无线专网	无线公网	中压PLC
参数值	1	0.75	0.5	0.25

2. 综合匹配分析

1）三遥业务

配电自动化三遥业务与通信技术匹配过程的组网结构、带宽、传输距离、实时性、可靠性、成本、技术成熟度及产业链、安全性等维度的价值因数分别如表3-8所示。由于配电自动化三遥业务对实时性、安全性要求较高，故价值因数取0.2，其他维度价值因数均取0.1。

表3-8 业务与通信技术匹配度排序表

业务指标分类	三遥价值因数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
组网结构及数据流向	0.1	0.75	0.75	1	0.5	0.5	0.25	0.25	0.25
带宽	0.1	0.125	0.25	0.875	0.5	0.625	1	0.75	0.375
传输距离	0.1	1	0.4	0.2	0.8	0.8	0.6	0.6	0.6
实时性（遥控）	0.2	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本，建设运维成本	0.1	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.1	0.83	0.67	0.5	0.33	0.17	1	1	1
信息安全	0.2	1	1	0.25	0.75	0.75	0.5	0.5	0.5
Z_i，i=1, 2, …, 8	1	0.8205	0.7	0.3895	0.625	0.6375	0.615	0.59	0.5525

根据以上分析，匹配值EPON＞工业以太网＞TD-LTE 230MHz＞TD-LTE 1800MHz＞2G＞3G＞4G＞中压PLC。

2）二遥业务

配电自动化二遥业务与通信技术匹配过程表的组网架构、带宽、传输距离、实时性、可靠性、成本、技术成熟度及产业链、安全性等维度的价值因数分别如表3-9所示。由于配电自动化二遥业务对成本因素敏感，故成本价值因数取0.3，其他维度价值因数均取0.1。

表3-9 业务与通信技术匹配度排序表

业务指标分类	二遥权重系数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
组网结构及数据流向	0.1	0.75	0.75	1	0.5	0.5	0.25	0.25	0.25
带宽	0.1	0.125	0.25	0.875	0.5	0.625	1	0.75	0.375
传输距离	0.1	1	0.4	0.2	0.8	0.8	0.6	0.6	0.6

续表

业务指标分类	二遥权重系数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
实时性	0.1	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本	0.3	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.1	0.83	0.67	0.5	0.33	0.17	1	1	1
安全性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
Z_i，$i=1$，…，8	1	0.72	0.59	0.38	0.62	0.67	0.73	0.70	0.66
		0.485	0.351325	0.3825	0.423	0.4195	0.335		

根据以上分析，匹配值2G>EPON>3G>TD-LTE 230MHz>4G>TD-LTE 1800MHz>中压PLC。

3. 匹配结果

配电自动化三遥业务，对通信网络的实时性、安全性要求较高，网络性能指标因素高于网络建设经济成本因素，兼顾技术成熟度和产业链完整性分析，优先采用光纤通信或无线专网通信。

配电自动化二遥业务，对通信网络的实时性、安全性要求相对较低，优先考虑网络建设经济成本，兼顾网络性能指标，宜优先采用无线公网、其他通信方式为辅的通信方式。在光纤或无线专网覆盖的区域，优先采用光纤或无线专网通信方式。

不同供电区域三遥和三遥业务分布不同，则不同供电区域建议采用不同的建设政策。

A+类区域以配电自动化三遥业务为主，优先采用光纤通信或无线专网。

A类区域包括三遥、二遥业务，应灵活选择光纤、无线或载波通信，“三遥”终端优先选择光纤通信和无线专网。

B类区域以二遥业务为主，C、D、E类区域采用二遥方式，考虑网络建设经济成本因素，宜采用无线公网承载为主、其他通信方式为辅的通信方式。

3.2.4　用电信息采集

业务特征分析表明，用电信息采集业务专变采集终端对通信网络的实时性、可靠性、安全性要求较高，网络性能指标因素高于网络建设经济成本因素，同时兼顾技术成熟度和产业链指标。集中器对时延要求较低，重点考虑经济建设成本，同时兼顾网络性能指标。

1. 业务与通信技术匹配

1）业务架构及数据流向

用电信息采集系统以省为单位部署，主站位于网省公司，采集终端非均匀遍布全省，采集终端与主站之间采用点对点双向通信。

中压PLC为电力特有通信技术，利用配电线路传输数据，网络拓扑与电网架构完全吻合；光纤专网借助随配电线路敷设的光缆传输数据，网络拓扑与电网架构基本吻合；无线专网为电力自建网络，专网专用，核心网部署在地市，基站部署在变电站等电力场所，业务数据在基站实现汇聚，网络拓扑与电网架构大致吻合；无线公网为租用网络，数据通过公网专线在地市汇聚，网络拓扑与电网架构无关。基于以上分析，业务架构与数据流向匹配度由高到低排序如表3-10所示。

表3-10　业务架构匹配度排序表

通信技术	中压PLC	光纤专网	无线专网	无线公网	备注
业务架构要求	电力特有，数据利用配电线路传输	光纤随配电线路敷设	根据需求自建基站，数据直接在变电站汇聚	租用网络，运营商汇聚数据，在省/市专线接入	与电网架构吻合
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

中压PLC、光纤专网、无线专网匹配遥控业务架构与数据流向要求，无线公网不满足。

2）带宽

目前主站每天召测1次采集终端数据，随着应用扩展，采集频率将会加快，根据调研情况可知，预计召测时间间隔为1h或15min。专变采集终端每天需传输数据量为6.14kbit，集中抄表终端（按照1000块电表计算）每天需传输数据量为5828kbit，分布式能源监控终端每天需传输数据量为5.82kbit，目前采用轮询机制，在规定时间段（6个小时）内将数据量上传至主站，速率按照要求自适应匹配，一般最低为1.2kbps，最高为40kbps。

按照业务速率自适应匹配要求，各类通信技术速率指标如下：2G无线公网传输速率为10～90kbps，中压PLC传输速率为10～100kbps，3G无线公网传输速率为30～700kbps，TD-LTE 230MHz无线专网传输速率为500kbps～1Mbps，TD-LTE 1800MHz无线专网传输速率为5～10Mbps，4G无线公网传输速率为5～10Mbps，工业以太网传输速率大于5/50Mbps（100/1000M带宽，按20个终端计算），EPON传输速率大于30Mbps（1.25Gbps共享，按32个终端计算）。通信技术最小速率与业务匹配度排序如表3-11所示。

表3-11 带宽参数匹配度排序表

通信技术	2G	中压PLC	3G	TD-LTE 230MHz	TD-LTE 1800MHz	4G	工业以太网	EPON	备 注
速率值	10～90kbps	10～100kbps	30～700kbps	1M带宽源：500kbps～1Mbps	5M带宽源：5～10Mbps	5～10Mbps	单终端≥5/50Mbps	单终端≥30Mbps	10.2kbps
排序结果	1	2	3	4	5	6	7	8	
匹配度参数	1	0.875	0.75	0.625	0.5	0.375	0.25	0.125	线性比例变化法：以最匹配为1，按照排序均分递减

无线公网2G、中压PLC匹配业务带宽要求，其他的通信技术可以提供更高带宽，但存在带宽资源浪费问题。无线公网性能受运营商网络负荷影响，速率波动较大，中压载波在干扰较多、信道不稳定的情况下带宽较低。

3）传输距离

变电站出线至台变的传输距离在20km范围内，EPON光纤通信技术传输距离小于20km，无线专网传输距离可根据需要进行区域覆盖，无线公网传输距离取决于运营商覆盖区域，工业以太网交换机技术传输距离大于20km，中压PLC技术传输距离为地埋小于2km、架空小于10km。各类通信技术传输距离与业务的匹配度由高到低排序如表3-12所示。

表3-12 传输距离匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备 注
距离	＜20km	根据选用光模块不同传输距离不同，为1～80km不等	自建基站覆盖区域，可根据需要	运营商网络覆盖区域	不考虑中继，地埋＜2km、架空＜10km	＜20km
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

EPON、无线专网、无线公网匹配业务带宽要求；工业以太网可覆盖更广区域；不考虑中继，中压PLC覆盖范围不满足要求。

4）实时性

用电信息采集系统遥控操作响应时间要求≤5s（包括两次主站到终端命令传输时间，一次终端到主站命令传输时间），数据召测响应时间要求＜15s。EPON光纤通信技术传输时延为1.5ms，工业以太网交换机网络传输时延为10ms，无线专网传输时延为30～300ms，无线公网传输时延为600ms～2s，中压PLC传输时延为0.3～3s。专变采集终端终端遥控操作实时性匹配度由高到低排序如表3-13所示。

表3-13　专变采集终端（含负控）遥控操作实时性匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　注
时延值	1.5ms	10ms	30～300ms	600ms～2s	0.3s～3s	＜1.7s
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

EPON、工业以太网、无线专网匹配遥控业务时延要求，其他通信技术不匹配。

集中抄表终端与分布式能源计量终端（非控类）目前没有具体时延要求，按照现场实测数据，各类通信技术均能满足业务要求。非控类终端遥控操作实时性匹配度由高到低排序如表3-14所示。

表3-14　非控终端数据采集实时性匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　注
时延值	1.5ms	10ms	30～300ms	600ms～2s	0.3～3s	＜1.7s
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

5）可靠性

用电信息采集对遥控正确率、采集成功率要求较高，均在95%以上。

光纤专网依靠光纤传输，不受电磁干扰和雷电影响，EPON系统中光分路器为无源器件，设备使用寿命长，系统具备抗多点失效的能力，“手拉手”保护组网模式光纤保护倒换时间≤100ms。工业以太网交换机同样采用光纤线路，系统的无故障工作时间＞17520h，单台交换机的环网恢复时间不超过50ms。光纤专网（EPON）数据采集一次成功率＞99%。

无线公网为租用网络，信道受天气、地形、网络负荷等因素影响，信号易受干扰，服务质量可变因素较多，尤其发生突发事件时，不能保证畅通，无线公网（GPRS）数据采集一次成功率＞97%。无线专网为自建网络，专网专用，需要专业技术人员开展网络优化，在基站覆盖范围内，理论上可靠性高于无线公网，无线专网（230数传电台）数据采集一次成功率＞97%，TD-LTE无线专网目前处于试点阶段，可靠性需进一步验证。中压载波易受电网环境干扰，信道稳定性较差，中压PLC数据采集一次成功率＞85%。各类通信技术可靠性匹配度由高到低如表3-15所示。

表3-15　可靠性匹配度排序表

通信技术	光纤专网	无线专网	无线公网	中压PLC	备　注
可靠性	一次成功率＞99%（EPON）	一次成功率＞97%（230电台）	一次成功率＞97%（GPRS）	一次成功率＞85%	遥控正确率、采集成功率等均大于95%

续表

通信技术	光纤专网	无线专网	无线公网	中压PLC	备注
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

光纤专网、无线专网、无线公网匹配遥控业务可靠性要求，中压PLC不匹配。

6）安全性

专变采集终端对安全性要求较高，集中器安全性要求相对较低。EPON、工业以太网交换机安全性较高，能满足专变采集终端安全性要求，无线专网、中压载波、无线公网匹配性较差。针对集中器，EPON、工业以太网交换机、无线专网、中压载波、无线公网均可以满足安全性要求。通信技术安全性匹配度由高到低排序如表3-16所示。

表3-16　安全性匹配度排序表

排序结果	1	2	3	4
通信技术	光纤专网	无线专网	无线公网	中压PLC
参数值	1	0.75	0.5	0.25

2. 综合匹配分析

1）专变采集终端（含负控）

用电信息采集业务专变采集终端（含负控）遥控操作响应与通信技术匹配过程的业务架构与数据流向、带宽、传输距离、实时性、可靠性、安全性、成本、技术成熟度及产业链等维度的价值因数分别如表3-17所示。由于遥控操作响应对实时性、可靠性要求较高，故实时性、可靠性价值因数取0.3，其他维度价值因数均取0.1。

表3-17　遥控操作与通信技术匹配度排序表

业务指标分类	权重系数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
组网结构与数据流向	0.1	0.75	0.75	1	0.5	0.5	0.25	0.25	0.25
带宽	0.1	0.125	0.25	0.875	0.5	0.625	1	0.75	0.375
传输距离	0.1	1	0.4	0.2	0.8	0.8	0.6	0.6	0.6
实时性	0.2	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.2	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本	0.1	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.1	0.83	0.67	0.5	0.33	0.17	1	1	1
安全性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
Z_i, i=1, ···, 8	1	0.82	0.70	0.39	0.63	0.64	0.62	0.59	0.55

根据以上分析，匹配值EPON＞工业以太网＞TD-LTE 230MHz＞TD-LTE 1800MHz＞2G＞3G＞4G＞中压PLC。

2）集中抄表终端

用电信息采集业务集中抄表终端与分布式能源监控终端（非控类终端）数据采集业务与通信技术匹配过程的业务架构与数据流向、带宽、传输距离、实时性、可靠性、安全性、成本、技术成熟度及产业链等维度的价值因数分别如表3-18所示，由于用电信息采集业务非控类终端主要考虑经济成本，故经济成本价值因数取0.4；对实时性、可靠性要求相对较低，故实时性、可靠性价值因数取0.05；其他维度价值因数均取0.1。

表3-18　数据采集业务与通信技术匹配度排序表

业务指标分类	权重系数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
组网结构及数据流向	0.1	0.75	0.75	1	0.5	0.5	0.25	0.25	0.25
带宽	0.1	0.125	0.25	0.875	0.5	0.625	1	0.75	0.375
传输距离	0.1	1	0.4	0.2	0.8	0.8	0.6	0.6	0.6
实时性	0.05	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.05	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本	0.4	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.1	0.83	0.67	0.5	0.33	0.17	1	1	1
安全性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
Z_i，i=1, 2, …, 8	1	0.67	0.53	0.37	0.62	0.68	0.78	0.76	0.72

根据以上分析，匹配值2G＞3G＞4G＞TD-LTE 230MHz＞EPON＞TD-LTE 1800MHz＞工业以太网＞中压PLC。

3. 匹配结果

用电信息采集业务专变采集终端对通信网络的实时性、可靠性、安全性要求较高，网络性能指标因素高于网络建设经济成本因素，同时兼顾技术成熟度和产业链指标。集中器对时延要求较低，重点考虑经济建设成本，同时兼顾网络性能指标。

专变采集终端对实时性、可靠性要求较高，无线公网时延波动性大，服务质量难以保障，载波易受环境干扰，稳定性较差，宜优先采用光纤或无线专网方式进行承载。

集中抄表终端和分布式能源监控终端对实时性、可靠性要求较低，考虑成本因素，宜优先选用无线公网，未来可能绘制用电动态曲线，信息量将显著增加，2G无线公网与载波速率将难以满足业务通信要求，宜优先采用4G无线公网；在已有光纤资源或无线专网覆盖的区域，可采用光纤或无线专网方式进行承载。

3.2.5　分布式电源

1. 业务与通信技术匹配

1）业务架构及数据流量

分布式电源的主站，即分布式能源监控系统或配网主站，位于地市调度中心。分布式电源的一体化监控装置随分布式电源部署，与主站之间采用点对多点双向通信。

中压PLC利用电力接线线路传输数据，网络拓扑与电网架构完全吻合；光纤专网借助随分布式电源接线线路敷设的光缆传输数据，网络拓扑与电网架构基本吻合；无线专网为电力自建网络，专网专用，核心网部署在地市，基站部署在变电站等电力场所，业务数据在基站实现汇聚，网络拓扑与电网架构大致吻合；无线公网为租用网络，数据通过公网专线在地市汇聚，网络拓扑与电网架构无关。基于以上分析，业务架构与数据流向匹配度由高到低排序如表3-19所示。

表3-19　业务架构匹配度排序表

通信技术	中压PLC	光纤专网	无线专网	无线公网	备　注
业务架构要求	电力特有，数据利用配电线路传输	光纤随配电线路敷设	根据需求自建基站，数据直接在变电站汇聚	租用网络，运营商汇聚数据，在省/市专线接入	与电网架构吻合
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

由表3-19可以分析出，中压PLC技术匹配度最高。

2）带宽

35/10kV分布式电源监控、电能质量监测信息采集频率类似配电自动化系统；分布式电源的计量信息采集是用电信息采集系统的一部分，采集频率与用电信息采集业务一致，以上通信技术都能满足要求。

35/10kV分布式电源终端单点接入的流量是42.3kbps，EPON、工业以太网交换机、无线专网（TD-LTE 230MHz、TD-LTE 1800MHz）可以很好地满足带宽要求。无线公网性能受运营商网络负荷影响，速率波动较大（2G网络速率约10～90kbps，3G网络速率约为30～700kbps，4G网络速率可达5～10Mbps）。在以最低速率匹配业务需求为优先原则进行评价时，35/10kV分布式电源终端单点接入与通信技术最小速率匹配度排序如表3-20所示。

表3-20　35/10kV分布式电源带宽参数匹配度排序表

通信技术	TD-LTE230MHz	TD-LTE 1800MHz	4G	工业以太网	EPON	3G	中压PLC	2G	备　注
速率值	1M带宽资源：500kbps～1Mbps	5M带宽资源：5～10Mbps	5～10Mbps	单终端≥5/50Mbps	单终端≥30Mbps	30～700kbps	10～100kbps	10～90kbps	42.3kbps

续表

通信技术	TD-LTE230MHz	TD-LTE 1800MHz	4G	工业以太网	EPON	3G	中压PLC	2G	备　注
排序结果	1	2	3	4	5	6	7	8	
匹配度参数	1	0.8	0.8	0.6	0.6	0.2	0.15	0.1	线性比例变化法：以最匹配为1，按照排序均分递减

380/220V分布式电源终端单点接入的流量是1.05kbps，与通信技术最小速率匹配度排序如表3-21所示。

表3-21　380/220V分布式电源带宽参数匹配度排序表

通信技术	2G	中压PLC	3G	TD-LTE 230MHz	TD-LTE 1800MHz	4G	工业以太网	EPON	备　注
速率值	10～90kbps	10～100kbps	30～700kbps	1M带宽资源：500kbps～1Mbps	5M带宽资源：5～10Mbps	5～10Mbps	单终端≥5/50Mbps	单终端≥30Mbps	1.05kbps
排序结果	1	2	3	4	5	6	7	8	
匹配度参数	1	0.875	0.75	0.625	0.5	0.375	0.25	0.125	线性比例变化法：以最匹配为1，按照排序均分递减

由表3-21可以分析出，35/10kV分布式电源终端单点接入时，TD-LTE230技术匹配度最高。2G、3G网络速率在运营商网络负荷较大时不满足带宽要求。中压载波在干扰较少、信道稳定的情况下，能满足带宽要求，在干扰较多、信道不稳定的情况下不满足带宽要求。380/220V分布式电源终端单点接入时，以上各种通信技术都能满足要求，2G技术匹配度最高。

3）传输距离

35kV分布式电源的接入传输距离一般在10～20km；10kV分布式电源的接入传输距离在配电网A+、A、B类区域不超过10km，EPON/无线通信/工业以太网交换机/中压载波都支持；C、D、E类区域为10～20km，部分区域达到数十千米；380/220V分布式电源的接入传输距离一般不超过20km。

在超过10km，不足20km传输距离以内，EPON、无线通信、工业以太网交换机都支持，中压载波无法满足需求。在10km以内，所有通信方式均满足。

因此整体来看，分布式电源终端单点接入通信距离小于20km，与通信技术传输最大距离匹配度排序如表3-22所示。

表3-22　传输距离匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　注
距离	＜20km	根据选用光模块不同传输距离不同，为1～80km不等	自建基站覆盖区域，可根据需要	运营商网络覆盖区域	不考虑中继，地埋＜2km、架空＜10km	＜20km 部分超过10km

续表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　注
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

由表3-22可以分析出，EPON、无线通信、工业以太网交换机匹配度较高，中压载波匹配度较低。

4）实时性

35/10kV分布式电源有分布式电源监控信息、电能质量监测、计量信息，“遥信”和“遥测”对光纤通信时延要求小于3s，“遥控”对光纤通信要求小于10s，EPON和工业以太网交换机都能满足；“遥信”和“遥测”对载波通信时延要求小于30s，“遥控”对载波的要求小于60s，中压载波可以满足；“遥信”和“遥测”对无线通信时延要求小于60s，无线通信都可以满足。电能质量监测、计量信息实时性要求低于监控信息实时性要求，以上技术都匹配。

380/220V分布式电源仅有计量信息接入，以上技术都能匹配。

可以看出，不同业务针对不同通信技术的实时性要求是不同的，因此本书以最小时延要求对分布式电源进行匹配。根据通信速率最小时延匹配业务可接受最大时延进行比对，且时延越小越优，排序结果如表3-23所示。

表3-23　遥控业务实时性匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　注
时延值	1.5ms	10ms	30～300ms	600ms～2s	0.3s～3s	＜1.5s
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

由表3-23可以分析出，在实时性方面，光纤通信匹配度最高。

5）可靠性

现有的分布式电源接入相关规范仅对业务系统可靠性提出要求，未对通信通道可靠性提出要求。

从设备可靠性角度35/10kV电压等级接入配电网的分布式能源站点，包含控制类业务，光纤网络不受电磁干扰和雷电影响，EPON系统中光分路器为无源器件，设备使用寿命长，系统可抗多点失效，“手拉手”保护组网模式光纤保护倒换时间≤100ms，可靠性高，匹配性好。工业以太网交换机同样采用光纤线路，系统的无故障工作时间＞17520h，单台交换机的环网恢复时间不超过50ms，可靠性高，匹配性好。光纤专网（EPON）数据采集一次成功率＞99%。

无线公网为租用网络，信道受天气、地形、网络负荷等因素影响、信号易受干扰，服务质量可变因素较多，尤其发生突发事件时，不能保证畅通。无线专网为自建网络，专网专用，需要专业技术人员开展网络优化，在基站覆盖范围内，理论上可靠性高于无线公网，TD-LTE无线专网目前处于试点阶段，可靠性需进一步验证。中压载波易受电网环境干扰，信道稳定性较差。各通信技术可靠性匹配度由高到低排序如表3-24所示。

表3-24　可靠性匹配度排序表

通信技术	光纤专网	无线专网	无线公网	中压PLC	备　注
可靠性	一次成功率＞99%（EPON）	一次成功率＞97%（230电台）	一次成功率＞97%（GPRS）	一次成功率＞85%	终端在线率、遥控成功率、遥信动作正确率等均＞95%
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

由表3-24可看出光纤专网、无线专网、无线公网匹配遥控业务可靠性匹配度较高，中压PLC匹配度较低。

6）安全性

光纤通信方式由于通信通道的封闭性，通过部署两套独立的通信设备可实现物理隔离，在通信设备上配置访问控制策略、划分VLAN等安全措施后，安全性相对较高。

无线通信本身固有的开放性使得它更容易受到监听、滥用等安全威胁，虽然随着无线通信技术体制的演进升级，采用了用户鉴权、加密等逐步增强的安全措施，但有限的网络带宽和终端资源限制了加密算法的类型和安全协议的开销等，尤其是无线公网方式无法实现物理隔离，安全性相对较低。通信技术安全性匹配度排序由高到低如表3-25所示。

表3-25　安全性匹配度排序表

排序结果	1	2	3	4
通信技术	光纤专网	无线专网	无线公网	中压PLC

35/10kV分布式电源对数据安全性要求高，适合采用自建光纤通信方式。380/220V分布式电源对数据安全性要求较低，适合采用无线通信方式。

2. 综合匹配分析

1）35/10kV分布式电源

接入35/10kV电压等级配电网的分布式能源站点业务与通信技术匹配过程的业务架构及数据流向、带宽、传输距离、实时性、可靠性、安全性、成本、技术成熟度及产业链等维度的价值因数分别如表3-26所示。由于分布式电源接入对可靠性和安全性要求较高，故可靠性和安全性价值因数取0.2，其他维度价值因数均取0.1。

表3-26　业务与通信技术匹配度排序表

业务指标分类	35/10kV业务价值因数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
业务架构及数据流向	0.1	0.75	0.75	1	0.5	0.5	0.25	0.25	0.25
带宽	0.1	0.6	0.6	0.15	0.8	1	0.1	0.2	0.8
传输距离	0.1	1	0.4	0.2	0.8	0.8	0.6	0.6	0.6
实时性	0.1	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.2	1	1	0.25	0.75	0.75	0.5	0.5	0.5
安全性	0.2	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本	0.1	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.1	0.83	0.67	0.5	0.33	0.17	1	1	1
Z_i, i=1, …, 8	1	0.868	0.755	0.322	0.67	0.69	0.535	0.545	0.605

2）380/220V分布式电源

接入380/220V电压等级配电网的分布式能源站点业务与通信技术匹配过程的业务架构与数据流向、带宽、传输距离、实时性、可靠性、安全性、成本、技术成熟度及产业链等维度的价值因数分别如表3-27所示。由于配电自动化三遥业务对实时性要求较高，故实时性价值因数取0.3，其他维度价值因数均取0.1。

表3-27　业务与通信技术匹配度排序表

业务指标分类	380/220V业务价值因数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
业务架构及数据流向	0.05	0.75	0.75	1	0.5	0.5	0.25	0.25	0.25
带宽	0.25	0.125	0.25	0.875	0.5	0.625	1	0.75	0.375
传输距离	0.1	1	0.4	0.2	0.8	0.8	0.6	0.6	0.6
实时性	0.05	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
安全性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本	0.25	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.1	0.83	0.67	0.5	0.33	0.17	1	1	1
Z_i, i=1, …, 8	1	0.62675	0.5295	0.44125	0.6105	0.66575	0.7925	0.73	0.63625

根据以上分析，接入35/10kV电压等级配电网的分布式能源业务，匹配值EPON＞工业以太网＞TD-LTE 230MHz＞TD-LTE 1800MHz＞4G＞3G＞2G＞中压PLC。

接入380/220V电压等级配电网的分布式能源业务，匹配值EPON＞工业以太网＞TD-LTE 230MHz＞TD-LTE 1800MHz/ 2G＞3G＞4G＞中压PLC。

3. 匹配结果

接入35/10kV电压等级配电网的分布式能源站点，业务类型包括遥控业务，时延要求小于6s，传输速率要求高于42.3kbps，技术指标因素高于经济因素，优先采用EPON或工业以太网交换机光纤专网。

窄带PLC传输时延为1～2s，宽带PLC传输时延约为400ms，物理层传输速率理论值为130kbps，满足遥控业务要求。但载波以电力线路为通信介质，传输特性时变性强，通道可靠性较差，会出现通信失败的现象，不适宜大规模组网部署。

TD-LTE 1800MHz无线专网传输时延约为30～50ms，在5MHz频谱带宽情况下终端传输速率为5Mbps，TD-LTE 230MHz无线专网传输时延约为1s，在1MHz频谱带宽情况下传输速率为1.76Mbps，可以满足遥控业务时延和传输速率要求。

无线公网时延波动性大，超出10s，不能满足遥控时延要求。

380/220V低压接入的分布式能源站点，业务信息主要为用电信息采集计量信息，业务终端数量多，离散分布，在终端通信接入网资源已覆盖区域，应充分利用已有资源实现覆盖；在终端通信接入网资源未覆盖区域，考虑经济成本，优先采用无线虚拟专网。

3.2.6 电动汽车充电站（桩）

1. 业务与通信技术匹配

1）业务架构及数据流向

电动汽车充电站（桩）为总部一级部署，主站位于上海灾备中心，终端分布无规律，一般处在市区、高速以及变电站附近，终端与主站之间点对点双向通信。

无线公网为租用网络，数据通过公网专线在省公司汇聚，网络拓扑与电网架构无关。无线专网为电力自建网络，核心网部署在省/市公司，基站部署在变电站等电力场所，业务数据在基站实现汇聚，网络拓扑与电网架构大致吻合。光纤专网借助随配电线路敷设的光缆传输数据，网络拓扑与电网架构基本吻合。中压PLC为电力特有通信技术，利用配电线路传输数据，网络拓扑与电网架构吻合。各通信技术业务架构匹配度排序由高到低如表3-28所示。

表3-28 业务架构匹配度排序表

通信技术	无线公网	无线专网	光纤专网	中压PLC	备注
业务架构要求	租用网络，运营商汇聚数据，在省/市专线接入	根据需求自建基站，数据直接在变电站汇聚	光纤随配电线路敷设，数据在变电站汇聚，终端沿配电线路部署	电力特有，数据利用配电线路传输，终端沿配电线路部署	终端至主站双向通信，不依赖电网架构

续表

通信技术	无线公网	无线专网	光纤专网	中压PLC	备　注
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

根据表3-28分析显示，无线网络匹配业务架构较好，其他的通信技术网络架构存在局限，匹配性较差。

2）带宽

根据测算，充电桩的通信带宽要求为4kbps。按单个充电桩终端的实时数据传输速率4kbps以及集中充电站10Mbps进行匹配，各类通信技术速率指标如下：2G无线公网传输速率为10～90kbps，中压PLC传输速率为10～100kbps，3G无线公网传输速率为30～700kbps，TD-LTE 230MHz无线专网传输速率为500kbps～1Mbps，TD-LTE 1800MHz无线专网传输速率为5～10Mbps，4G无线公网传输速率为5～10Mbps，工业以太网传输速率大于5/50Mbps（100/1000Mbps带宽，按20个终端计算），EPON传输速率大于30Mbps（1.25Gbps共享，按32个终端计算）。通信技术最小速率与业务匹配度排序如表3-29所示。

表3-29　充电桩带宽参数匹配度排序表

通信技术	2G	中压PLC	3G	TD-LTE 230MHz	TD-LTE 1800MHz	4G	工业以太网	EPON	备　注
速率值	10～90kbps	10～100 kbps	30～700kbps	1M带宽资源：500kbps～1Mbps	5M带宽资源：5～10Mbps	5～10 Mbps	单终端≥5/50 Mbps	单终端≥30 Mbps	4kbps
排序结果	1	2	3	4	5	6	7	8	
匹配度参数	1	0.875	0.75	0.625	0.5	0.375	0.25	0.125	线性比例变化法：以最匹配为1，按照排序均分递减

根据表3-29分析显示，无线公网2G、中压PLC以及3G匹配业务带宽要求，其他的通信技术可以提供更高带宽，但存在带宽资源浪费。

集中充电站带宽参数匹配度如表3-30所示。

表3-30　集中充电站带宽参数匹配度排序表

通信技术	EPON	工业以太网	TD-LTE 1800MHz	4G	TD-LTE 230MHz	中压PLC	3G	2G	备　注
速率值	单终端≥30 Mbps	单终端≥5/50 Mbps	5M带宽资源：5～10Mbps	5～10 Mbps	1M带宽资源：500kbps～1Mbps	10～100 kbps	30～700kbps	10～90kbps	10Mbps
排序结果	1	2	3	4	5	6	7	8	
匹配度参数	1	0.875	0.75	0.625	0.5	0.375	0.25	0.125	线性比例变化法：以最匹配为1，按照排序均分递减

根据表3-30分析显示，EPON、工业以太网匹配业务带宽要求，其他通信技术可以提供的带宽较低，匹配性较差。

3）传输距离

充电桩的距离一般在市区范围内，距离配电台区较近；集中充电站与上联变电站/开闭所距离均在2～5km。

无线专网传输距离可根据需要进行区域覆盖，无线公网传输距离取决于运营商覆盖区域，EPON光纤通信技术传输距离小于20km，工业以太网交换机技术传输距离大于20km，中压PLC技术传输距离为地埋小于2km、架空小于10km。各类通信技术传输距离与业务的匹配度由高到低排序如表3-31所示。

表3-31　业务传输距离匹配度排序表

通信技术	无线专网	无线公网	中压PLC	EPON	工业以太网	备　注
距离	自建基站覆盖区域，可根据需要	运营商网络覆盖区域	不考虑中继，地埋＜2km、架空＜10km	＜20km	根据选用光模块不同传输距离不同，为1～80km不等	距配电台区距离较近
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

根据表3-31分析显示，无线网络、中压PLC以及EPON匹配业务传输距离较好，工业以太网交换机技术提供传输距离较远，存在资源浪费。

4）实时性

充电桩数据业务对实时性要求一般，要求时延小于5s，在采集间隔2min内将数据上传即可。EPON光纤通信技术传输时延为1.5ms，工业以太网交换机网络传输时延为10ms，无线专网传输时延为30～300ms，无线公网传输时延为600ms～2s，中压PLC传输时延为0.3～3s。遥控业务实时性匹配度由高到低排序如表3-32所示。

表3-32　遥控业务实时性匹配度排序表

通信技术	EPON	工业以太网	无线专网	无线公网	中压PLC	备　注
时延值	1.5ms	10ms	30～300ms	600ms～2s	0.3s～3s	＜5s
排序结果	1	2	3	4	5	
匹配度参数	1	0.8	0.6	0.4	0.2	线性比例变化法：以最匹配为1，按照排序均分递减

根据表3-32分析显示，各类技术均能较好地匹配业务实时性要求。

5）可靠性

电动汽车充电站（桩）业务在采集周期内满足99%以上可靠性要求。

光纤专网依靠光纤传输，不受电磁干扰和雷电影响，EPON系统中光分路器为无源器件，设备使用寿命长，系统具备抗多点失效的能力，“手拉手”保护组网模式光纤保护倒换时间≤100ms。工业以太网交换机同样采用光纤线路，系统的无故障工作时间＞17520h，单台交换机的环网恢复时间不超过50ms。光纤专网（EPON）数据采集一次成功率＞99%。

无线公网为租用网络，信道受天气、地形、网络负荷等因素影响、信号易受干扰，服务质量可变因素较多，尤其发生突发事件时，不能保证畅通。无线专网为自建网络，专网专用，需要专业技术人员开展网络优化，在基站覆盖范围内，理论上可靠性高于无线公网；TD-LTE无线专网目前处于试点阶段，可靠性需进一步验证。中压载波易受电网环境干扰，信道稳定性较差。各通信技术可靠性匹配度由高到低排序如表3-33所示。

表3-33　可靠性匹配度排序表

通信技术	光纤专网	无线专网	无线公网	中压PLC	备　注
可靠性	一次成功率＞99%（EPON）	一次成功率＞97%（230电台）	一次成功率＞97%（GPRS）	一次成功率＞85%	终端在线率、遥控成功率、遥信动作正确率等均大于95%
排序结果	1	2	3	4	
匹配度参数	1	0.75	0.5	0.25	线性比例变化法：以最匹配为1，按照排序均分递减

光纤专网、无线专网、无线公网匹配电动汽车充电站（桩）业务可靠性要求，中压PLC不匹配。

6）安全性

光纤通信方式由于通信通道的封闭性，通过部署两套独立的通信设备可实现物理隔离，在通信设备上配置访问控制策略、划分VLAN等安全措施后，安全性相对较高。

无线通信本身固有的开放性使得它更容易受到监听、滥用等安全威胁，虽然随着无线通信技术体制的演进升级，采用用户鉴权、加密等逐步增强的安全措施，但有限的网络带宽和终端资源限制了加密算法的类型和安全协议的开销等，尤其是无线公网方式无法实现物理隔离，安全性相对较低。通信技术的安全性匹配度由高到低排序如表3-34所示。

表3-34　安全性匹配度排序表

通信技术	光纤专网	无线专网	无线公网	中压PLC
排序结果	1	2	3	4

2. 综合匹配分析

1）充电桩

充电桩业务与通信技术匹配过程的业务架构与数据流向、带宽、传输距离、实时性、可靠性、安全性、成本、技术成熟度及产业链等维度的价值因数分别如表3-35所示。考虑充电桩业务对经济成本及产业链完整因素敏感，故成本、技术成熟度及产业链完整价值因数取0.2，其他维度价值因数均取0.1。

表3-35　充电桩业务需求与通信技术匹配度排序表

业务指标分类	价值因数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
业务架构及数据流向	0.1	0.5	0.5	0.25	0.75	0.75	1	1	1

续表

业务指标分类	价值因数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
带宽	0.1	0.125	0.25	0.875	0.5	0.625	1	0.75	0.375
传输距离	0.1	0.4	0.2	0.6	1	1	0.8	0.8	0.8
实时性	0.1	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
安全性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本	0.2	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.2	0.83	0.67	0.5	0.33	0.17	1	1	1
Z_i, i=1, …, 8	1	0.6685	0.575	0.3765	0.635	0.6475	0.82	0.795	0.7575

根据以上分析，匹配值2G＞3G＞4G＞EPON＞TD-LTE 230MHz＞TD-LTE 1800MHz＞工业以太网＞中压PLC。

2）充电站

充电站业务与通信技术匹配过程的业务架构与数据流向、带宽、传输距离、实时性、可靠性、安全性、成本、技术成熟度及产业链等维度的价值因数分别如表3-36所示，由于集中充电站业务对带宽以及可靠性要求较高，故带宽和可靠性价值因数取0.2，其他维度价值因数均取0.1。

表3-36　集中充电站业务需求与通信技术匹配度排序表

业务指标分类	价值因数	光纤通信		中压PLC	无线专网		无线公网		
		EPON	工业以太网		TD-LTE 1800MHz	TD-LTE 230MHz	2G	3G	4G
业务架构及数据流向	0.1	0.5	0.5	0.25	0.75	0.75	1	1	1
带宽	0.2	1	0.875	0.375	0.75	0.5	0.125	0.25	0.625
传输距离	0.1	0.4	0.2	0.6	1	1	0.8	0.8	0.8
实时性	0.1	1	0.8	0.2	0.6	0.6	0.4	0.4	0.4
可靠性	0.2	1	1	0.25	0.75	0.75	0.5	0.5	0.5
安全性	0.1	1	1	0.25	0.75	0.75	0.5	0.5	0.5
成本	0.1	0.5	0.33	0.17	0.67	0.83	1	1	1
技术成熟度及产业链	0.1	0.83	0.67	0.5	0.33	0.17	1	1	1
Z_i, i=1, …, 8	1	0.823	0.725	0.322	0.71	0.66	0.595	0.62	0.695

根据以上分析，匹配值EPON＞工业以太网＞TD-LTE 1800MHz＞4G＞TD-LTE 230MHz＞3G＞2G＞中压PLC。

3. 匹配结果

充电桩是电动汽车服务网络的末端充电设施，数量多，位置分散，对安全性、实时性要求一般，应首先考虑网络建设成本。当充电桩所在区域具备终端通信接入网络资源时，可采用自建终端通信接入网络资源实现接入；当充电桩所在区域不具备终端通信接入网络资源时，采用无线公网接入车联网平台。

集中充电站由大量充电桩组成，对带宽及可靠性要求较高，网络性能指标高于网络经济建设成本，优先采用EPON或工业以太网交换机；保证带宽资源情况下，可考虑自建TD-LTE 1800MHz无线专网实现覆盖。

3.2.7　扩展业务匹配

1. 移动巡检

移动巡检业务需要实现巡检终端与巡检中心之间的通信，传输的数据包括文字、图片、视频等多种形式，带宽要求为：语音业务8～64kbps，视频业务384kbps～2Mbps，数据业务64kbps～2Mbps，语音和视频类业务对时延和可靠性要求较高。在无线专网覆盖区域优先采用无线专网，其他区域可以采用无线公网。

2. 配网抢修

配电抢修业务用于采集和传输配电故障现场的语音、图像、视频信息，传输速率需求约为4Mbps，时延要求为百毫秒级。在无线专网覆盖区域优先采用无线专网，其他区域适合使用4G无线公网。

3. 配电设备/环境状态监测

目前试点情况对带宽要求较低，实时性要求不高，单个接入点的速率需求约为几千比特每秒，传输时延为秒级，各种通信方式都可以匹配。未来规模化部署时，配电监测点数量庞大，监测位置分布分散，建议在无线专网覆盖区域优先采用无线专网，其他区域采用无线公网。

4. 电能质量监测

电能质量监测要求带宽高于1Mbps，在电力光纤/无线专网覆盖范围内优先使用光纤/无线专网，其他区域适合使用3G/4G无线公网。

5. 无人机巡检

无人机通信系统主要实现无人机遥控信号、巡检图像与遥控操作台的信息传输。遥控操作速率为100kbps以内，实时性、可靠性要求较高。巡检图像传输速率为2Mbps以上，实时性、可靠性要求较高，传输距离较远。无人机与地面控制站之间为厂商自定通信方式，不做业务与通信方式匹配分析。

6. 机器人巡检

机器人巡检数据类型包括图像、设备诊断等信息，数据传输速率要求大于2Mbps，对通信时延、可靠性要求较高。变电站内巡检一般选择WiFi技术组网。在无线专网覆盖区域可选用无线专网进行承载，其次为4G无线公网。

7. 基建现场视频监控

施工现场视频监控系统为临时性部署，对实时性、可靠性安全要求较低，在光纤专网与无线专网覆盖区域，优先选用光纤专网或无线专网进行业务承载，最后可选用3G/4G无线公网承载（考虑经济成本，仅传输图片）。

8. 智能家居

智能家居业务用于传输家电、语音、家庭安防等信息，传输速率约为1～4Mbps，传输时延为百毫秒级，适宜采用光纤通信技术。

9. 智能营业厅

接入网实现实体营业厅、互动终端营业厅的视频监控、柜台终端和自助服务终端、独立布置的自助终端和车载移动营业厅的通信接入，承载用户档案、用电信息、变更业务、缴费业务及服务管理等数据和视频业务，视频监控对带宽要求最高。实体营业厅、互动终端营业厅优先使用光纤专网接入，独立布置的自助终端优先通过光纤或无线专网接入，车载移动营业厅通过无线专网接入，手机营业厅、短信营业厅、网上营业厅可以通过电力专用VPN网络专线接入。

3.3 总　　结

本章主要介绍两方面，首先从10kV接入网和0.4kV接入网两部分对当前接入网的网络建设现状进行介绍，内容涉及光缆及设备建设现状、接入站点覆盖现状以及存在的问题。

终端通信接入网承载配电自动化、用电信息采集、分布式电源、电动汽车充电站、营业场所接入等业务，主要采用的通信技术包括光纤、电力线载波、无线公网和无线专网等，实现了业务终端通信全覆盖。但是目前接入网存在网络建设分散、通信资源利用率低、接入网技术政策不够完备等问题，需要进行深入的技术论证并完善适配业务的技术政策。然后又对不同业务进行了分析，将业务与通信技术进行匹配，提出了各种业务在不同场景下最合适的通信技术。

第4章
规划和运维技术需求分析



4.1 终端通信接入网规划技术需求分析

4.1.1 EPON规划

EPON带宽分配机制通常分为两种：静态带宽分配和动态带宽分配。在静态带宽分配中，OLT每周期分配给各ONU中各T-CONT的带宽是固定的，不随带宽请求量的变化而变化。这种分配方式简单明了，但是存在很多的缺陷。首先，该分配方式最大的不足在于静态带宽分配不能有效利用系统带宽，特别是当请求带宽与实际分配带宽的差距很大时，带宽利用率很低。其次，带宽分配机制需要区分和识别不同种类的数据流，并基于优先级，为每种数据流提供不同的服务，而静态带宽分配机制不能满足该需求。同时，有一些数据流对带宽和QoS有特殊的要求，静态带宽分配不能满足其要求。而动态带宽分配机制根据各ONU每周期的带宽请求分配带宽，灵活地将带宽分配给各T-CONT，能够更有效地利用带宽，满足各类数据流的业务需求。并能在对网络产生很小影响的情况下，灵活增加用户数量。因此，其较之于静态带宽分配来说，动态带宽分配机制更适用于实际应用。

传统的T-DBA（Two-levels DBA）算法在PON层根据服务等级协议SLA（Service Level Arrangement）分配不同的加权系数，以保证高优先级用户的带宽需求。而在ONU内部，高优先级业务可直接分得固定带宽，中低优先级业务则按照比例分配剩余带宽，该算法保证了高优先级用户及高优先级业务的需求，但无法根据网络实时情况灵活分配带宽，容易出现部分优先级业务带宽浪费，而另一部分优先级业务带宽不够的情况，造成带宽浪费或时延增加等问题。C-DBA是基于T-CONT并带有上行报告过程的算法。它对T-CONT1业务进行固定带宽分配；T-CONT2业务则采用确保带宽分配方式，即最大限度上满足其所有的上报需求；T-CONT3业务为先对它进行一个最小保证带宽分配，然后再将剩余T-CONT3请求与T-CONT4的请求一起分配，若带宽不够，按权重分给各个请求量。该算法保证了高优先级业务的需求，但固定带宽在重负载条件下的高带宽需求会造成轻负载条件下大量的带宽浪费，二者无法同时避免，无法满足低优先级带宽的算法公平性要求。

EPON网络作为一个点到多点式的结构，在上行方向上，所有的ONU共享同一个上行

信道，资源分配即带宽分配问题必然是研究的重点。共享的上行信道带宽也就是EPON每秒所能传输的最大数据量，目前其最大的通信容量为1Gbps。有了这样的带宽限制，在EPON网络上，所有的用户就不能获得无限制的带宽分配，不能每时每刻获得按需分配的带宽。因此在不同用户，也就是EPON的ONU之间的带宽分配必然需要考虑到公平性问题。

本章提出一种基于双分区的自适应优先级调度的动态带宽分配机制（APS-BDBA）来提高EPON支持多业务的能力。在ONU内，A-DBA机制将ONU的带宽分配过程分成两个部分。首先是动态分配高优先级，即T-CONT1和T-CONT2的带宽，T-CONT1采用固定带宽分配，T-CONT2采用带有流量预测的分配方式。第一部分的带宽分配完成后，再进行第二部分带宽请求及分配。第二部分的分配是针对低优先级业务的T-CONT3及T-CONT4，这样可以尽力消除等待时间间隔的问题，减少带宽浪费。而在各ONU之间，该技术设计了一个自适应优先级调度机制，该机制满足最高优先级业务流的最小时延要求。由于将分配分成两部分完成，减少了T-CONT3及T-CONT4业务的部分等待时间，该技术能够在一定程度上降低包时延。

4.1.2 无线专网规划

1. 非对称覆盖补偿技术

在基站失效之前，周围补偿基站会扩展其覆盖范围，保证基站失效后其覆盖区域不会出现盲区，并且考虑到补偿基站的负载分配不均衡性，最佳的覆盖补偿应该结合补偿基站的负载情况。以往的研究工作为了简化模型，都没有考虑到非对称的补偿方式，本项目组研究有别于传统覆盖补偿的非对称覆盖补偿策略，具体覆盖调整流程如图4-1所示。

① 由基站控制器（BSC）检测网络的整体业务负载情况，如果整体业务流量低于设定的低门限阈值D_{th}，且整体业务流量处于下降趋势时，则触发覆盖补偿流程，收集所需调整基站，即低负载基站的负载状况和周围基站的负载状况，包括业务容量以及用户所在位置等信息。

② 当BSC收集到基站信息之后，计算周围基站是否可以接受所有流量。如果周围基站不能接受所有流量，那么BSC返回监控状态，继续监控网络负载情况，而不采取覆盖调整措施。如果可以接受所有流量，那么根据用户位置将流量分配给多个基站，实现分流，但是每个接受基站在接受负载后仍然需要保持非高负载的状况，否则，返回监控状态。这么做是为了保证网络不会因为基站的失效而导致局部的负载过高、服务质量变差。

③ 在计算得到最佳的接收组合后，失效基站要求在一定的时间段内逐渐降低其发射功率，从而使覆盖区域的业务能够平滑转移。同时接收流量的基站调整其覆盖范围，进行覆盖补偿，然后将失效基站的业务转移至补偿基站。在基站进入休眠之后，休眠的基站不

再接收新业务接入。

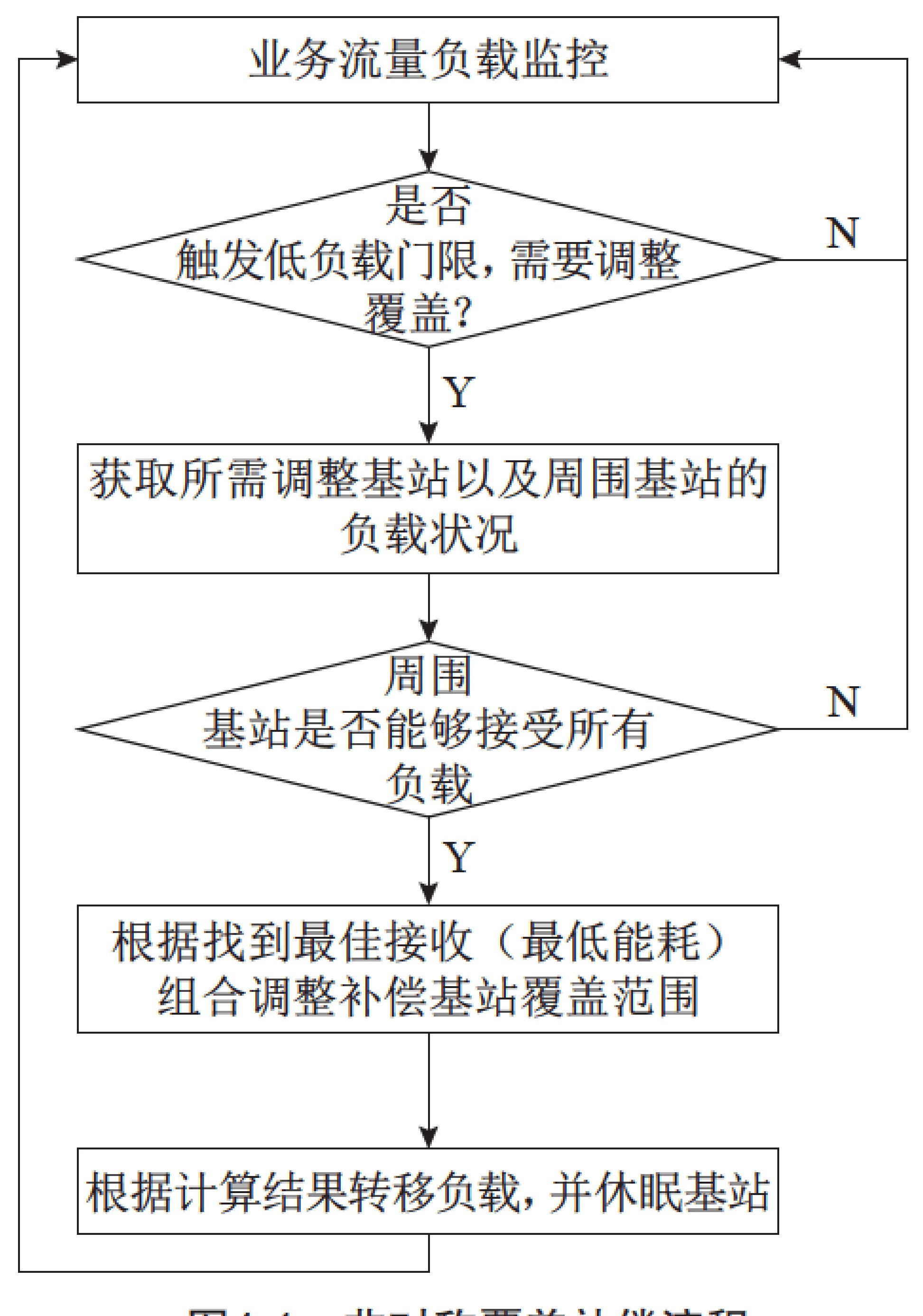


图4-1 非对称覆盖补偿流程

最终覆盖情况如图4-2所示。图中基站A是失效基站，左图表示失效前的覆盖情况，右图表示失效后的覆盖情况。

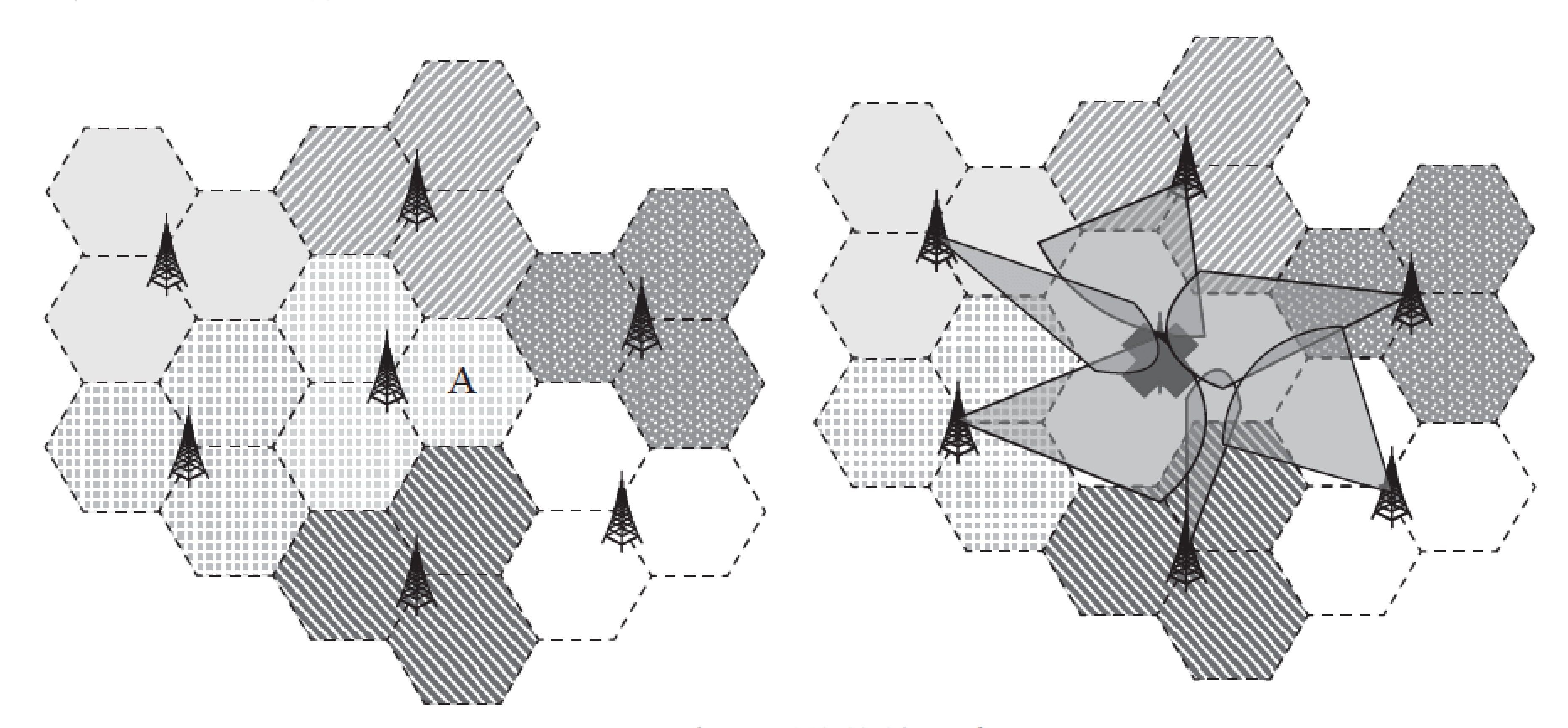


图4-2 扇区覆盖补偿示意图

2. 动态无线资源管理技术

异构融合将会成为终端通信接入网无线专网规划的主要特征，除此之外，智能化也是其重要特征之一。为了实现网络的交互访问，异构融合网络需要在现有的无线技术和网络设施的基础上，增加统一的移动管理机制、控制平面、网络设备以及控制系统的资源化。其中3GPP组织提出的SAE（系统架构演进）已经初步实现了异构网络融合的功能，能够

使不同的无线接入网实现互连，从而在网络的宏观层次实现统一管理。网络智能化是指网络能够随时实现对外界环境的感知，并且根据感知到的网络状况来进行响应和动态自适应环境的变化。无线认知网络正是符合这些要求的一种网络，其通过自身感知学习功能与复杂的无线环境实现交互来改变网元属性，从而实现异构环境下适应无线网络的动态变化。

接入选择作为异构融合网络中无线资源管理的一个重要组成部分，是影响异构融合系统资源利用率的首要因素。异构融合网络的接入选择要解决的主要问题就是如何综合利用不同无线通信网络的特点，在保证业务服务质量的情况下，提高异构网络的资源利用率。为了提高用户的QoS体验，优化系统资源调度，异构无线网络的接入选择不再是局限于单一属性的决策问题，而是面向用户、网络和终端等各层次特性及需求的多属性决策问题，必须全面考虑各种判决参数，如用户喜好、业务需求、网络安全、网络覆盖、可用网络资源和终端的能力与尺寸等。

4.1.3　工业以太网规划

终端通信接入网业务对时延及其可靠性非常敏感。基于终端通信接入网业务对网络性能的特殊需求，以及针对这些QoS需求工业以太网协议的改进方法分析，可以看到工业以太网的拓扑设计问题具有区别于其他网络拓扑设计问题的一些特点。

① 对实时性的需求更关心所有数据流的端对端时延性能，而不是平均时延性能。业务产生的每个数据流经过工业以太网时必须满足一定的时延约束，因此工业以太网的拓扑设计是一个多约束的优化问题。

② 快速冗余恢复需求，要求网络拓扑设计时考虑对快速冗余恢复协议的支持。本项目组考虑了基于环冗余的网络拓扑设计。

③ 实时性与可靠性需求要求在拓扑设计时同时考虑物理拓扑设计及其网络配置的逻辑拓扑。工业以太网的可靠性由网络的物理拓扑决定，而实时性能主要取决于网络配置的生成树逻辑拓扑。因此工业以太网的拓扑设计问题从数学上看是一个双层规划问题，包括物理拓扑和逻辑拓扑设计。

根据不同业务需求，其对应的工业以太网设计着重优化其中一个指标，双目标或者多个指标。根据设计解决问题的侧重点，工业以太网设计可以分成单目标或者多目标优化问题。由于现场具有计算和通信功能的智能设备越来越多，设备之间的信息交换也越来越多，工业以太网的拓扑设计问题的规模也随之增加。网络拓扑的设计方法要满足不同规模的工业应用需求。

4.2 终端通信接入网运维技术需求分析

4.2.1 运维模式

一般的通信接入网网管运维的结构模式在国际上主要分为3 类：集中式网络管理、分级式网络管理和分布式网络管理。

我国终端通信接入网起步较晚，没有统一的标准，而且网络结构复杂、通信方式多样、通信终端种类繁多且覆盖面广，管理难度非常大，目前多采用分布式网管运维体系。分布式网管运维体系的优点是灵活性强、成本低，目前电力通信接入网的多样性适合窄带及宽带多业务接入网的网络系统，便于网络升级。

世界各大公司都支持分布式网管运维模式，当前分布式网管运维模式的框架一般采用的模式主要有公共对象需求代理人结构（Common Object Request Broker Architecture，CORBA）、分布计算环境/分布管理环境、分布式公共对象模型（Distributed Common Object Model，DCOM）等。其中 CORBA 在国际上被优先推荐和采用，分布结构对象和框架的运用使得其可采用不同的供应商并跨越不同的操作系统和网络。CORBA还可以对所有对象实施操作，且同时完全不知道它们采用何种语言以及它们所处的位置。这一优点使其能够在未来复杂的通信信息网络中发挥极其重要的作用。我国电力系统行业，已经开展适于分布式网管运维系统的CORBA 等框架结构研究，并且正在开展相关系列标准的制定工作。

4.2.2 运维技术需求分析

1. 网络探针技术

1）探针系统

终端通信接入网运维中的流量监管不足的问题，可采用布置网络探针的方法进行合理解决。网络探针是一种未得到广泛应用的数据采集技术。数据包捕获、过滤、分析等功能都在“探针”上实现，分析的结果存储在探针的内存或磁盘之中，也可通过探针发送到后台数据库再次分析并存储。具体的前端展现依赖与之对应的软件设计。

硬件探针、服务器和后续分析程序三个模块构成一般的探针系统，如图4-3所示。

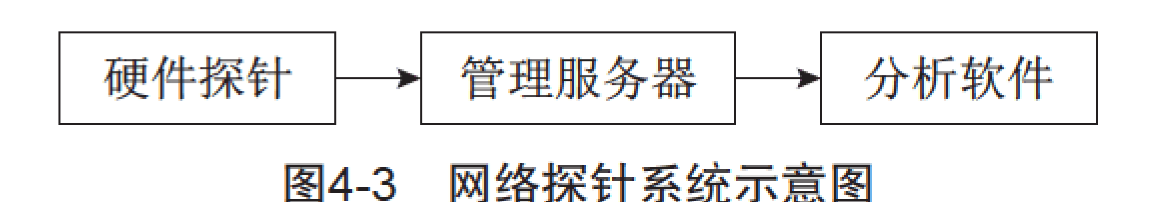


图4-3 网络探针系统示意图

① 硬件探针也是目前较主流的流量获取设备，它是通过串接或者旁接在设备或链路中获取网络流量的，将进出设备或端口的流量传递给分析服务器，具备强大的网络流量捕捉能力，可以将网络流量捕获并直接存储到硬盘上，流量存储的性能高达1800Mbps，并可以提供全七层协议解码能力。硬件探针部署方式是利用分光或镜像端口进行数据分类、过滤，上传汇聚至中心服务器的数据库，作为存储以及统一调用。

② 服务器由流量采集、管理程序和数据库构成。流量采集程序可以收集各个探针提供的数据流，并且对数据流进行解包，统计汇总，将数据存储在数据库中；探针与采集服务器利用特有的通信协议进行数据传输，并且采用主动上报的方式，一般采用安全性较高的 UDP 方式作为传输协议。管理程序则采用了 TCP 专门的高层通信协议，对探针设备和策略进行管理，可以直接对探针进行监控指标及维护策略下发；数据库可以满足对结构化数据的存储，并提供分析查询及搜索操作。

③ 流量分析应用程序可以按照任意条件从数据库中提取所关注的数据信息，从而方便地为统计报表、图表提供相关的统计信息。

如何在网络中部署探针也是采用探针技术的一个重要问题，主要是根据将网络流量有效测量点选择问题转化为求给定无向图中的最小顶点覆盖问题或最小弱顶点覆盖问题，如求解弱顶点覆盖集的贪婪秩算法、弱化的贪心算法等。刘湘辉等提出的一个求解最小弱项顶点覆盖集的近似算法不需要了解网络的拓扑信息，并且能够找到部署节点的更小的有效测量节点，是一种有效的探针节点选择方法。

2）现有探针类型以及主要支撑技术

（1）探针类型和用途

目前探针主要包括SNMP/RMON探针、NetFlowlsFlow探针和数据采集探针。

- SNMP/RMON探针

SNMP探针一般由软件实现的流量监测系统作为SNMP的管理者（Manager），路由器等设备充当SNMP的代理（Agent）。管理者定期向Agent发送SNMP请求snmpwalk，从Agent获取相关的流量信息。RMON协议是对SNMP标准的扩展，定义了远程监视的标准功能以及远程监控代理的接口，主要用于对一个网段乃至整个网络数据进行采集和测量。

- NetFlowlsFlow探针

NetFlow是Cisco公司开发的专用流交换技术，集成在Cisco的各类路由器和交换机内，同时也可用于记录流量统计信息。sFlow也是一种嵌入在路由器或交换机内的基于抽样的流量监测技术。

- 数据采集探针

数据采集探针是专门用于获取网络链路流量数据的硬件设备。硬件架构的数据采集探针是为了流量监测的目的而专门设计的技术方案，能够做到高速端口的线速流量采集，提供对GE甚至 2.5G POS链路的支持。

表4-1所示为不同探针类型的比较。

表4-1 不同探针类型比较

探针类型	主要厂商和产品	存在的缺点
SNMP/RMON探针	HP Openview、Cisco Works 2000、Nortel Optivity等	只能实现简单的网络测量数据的获取，实时流量的分析性能差，不能进行故障分析，不支持历史数据的存储、网络协议解码等功能的实现
NetFlowlsFlow探针	Cisco Flow Collector、Arbor Peakflow、CAIDA cfowd、FlowScan、Genie NTG等	特定于厂商的设备，部署复杂，价格昂贵，实时性较差等
数据采集探针	NetScout Probe、Sniffer硬件探针	特定于具体的网络的实现，费用较高，部署复杂

（2）WSDM技术

Web服务分布式管理（Web Services Distributed Management，WSDM）是一种技术规范，定义了用于管理网络资源（如探针、路由器和服务）和Web服务（用于支持网络功能）的系统的方法、结构和规范。此外，还可以使用WSDM管理支持业务应用程序的Web服务。WSDM是一个用于描述特定设备、应用程序或者组件的管理信息和功能的标准，其能够在整个环境中应用一个共同管理界面，允许不同厂商的管理软件更加轻松地实现相互操作，同时实现端到端的管理，甚至跨企业管理。WSDM为使用Web服务来建立管理应用奠定了基础，还能提供一系列设备来管理资源。

如果所有探针设备、服务、组件的管理信息和功能遵循WSDM标准，则通过Web服务能实现对接入网全面的监控和管理。目前面临的主要问题是，各个厂商的产品大都有自己的特色，执行部分的WSDM标准。

2. 流量分析技术

目前前沿流量分析技术包括基于SNMP的流量分析技术，基于网络探针的流量分析技术，基于实时抓包的流量分析技术和基于流的流量分析技术。

基于SNMP的流量分析技术仅能对网络设备端口的整体流量进行分析，可以获得设备端口的实时或者历史的流入/流出带宽、丢包、误包等性能指标，但无法分析具体的用户流量和协议组成。通过扩展实现RMON和RMONⅡ，该方法可在一定程度上（网络2层到4层）实现有限的端到端通信会话数据分析、TopN用户统计等功能。因其具有实现简单、标准统一、接口开放的特点，被业界广泛采用。

基于网络探针（Probe）的流量分析技术，其数据抓包、分析和统计等功能一般都在网络“探针”上以硬件方式实现，分析的结果存储在探针的内存或磁盘之中，具体的前端展现依赖与之对应的专门软件。因此具有效率高、可靠性高、高速运行不丢包的特点。这种方式可深入地对网络2层、3层甚至7层的特性进行详细分析。

基于实时抓包的流量分析技术提供详细的从物理层到应用层的数据分析。但该方法主要侧重于协议分析，而非用户流量访问统计和趋势分析，仅能在短时间内对流经接口的数据包进行分析，无法满足大流量、长期的抓包和趋势分析的要求。

基于流（Flow）的流量分析技术，目前主要有两种：sFlow和NetFlow。sFlow是由InMon、HP和Foundry Networks联合开发的一种网络监测技术，它采用数据流随机采样技术，可以适应超大网络流量（如大于10Gbps）环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题。

采用以上前沿高效的流量分析技术，能有效缩短流量分析的时间，减少运维人员工作量，同时为后续故障定位做好准备工作。

3. 故障定位技术

终端通信接入网故障检测与定位技术主要基于主动探针探测技术，该研究分为三个部分：①探针部署位置的选择；②探测路径的选择；③基于主动探测的故障诊断。其中探测路径的选择又分为两部分：故障检测探测的选择和故障定位探测的选择。

1）用于故障探测的主动探针选择技术

检测网络中是否存在故障是故障检测的目的，因此所选的测试路径需要满足覆盖网络中的所有节点。由探测站点向其他所有节点产生的探测路径便形成了所有可用探测集，在故障检测探测阶段，需要在可用探测集合中选择出一部分探测路径作为故障检测集合，故障检测集合的选取需满足以下条件：

① 网络中的所有节点都要被所选的测试路径覆盖。

② 形成尽量少的测试路径。

故障检测的探测选择问题其基本方法是基于贪心算法的近似算法，目前常见的贪心策略求解思路有两种：一是贪心增加算法，即设初始化探测集合为空，不断选取能够覆盖最多的尚未被覆盖节点的探测，直到所有节点都被覆盖；二是贪心减少算法，即将所有探测的全集设为初始化探测集合，不断尝试删除某个探测，只需判定该探测的删除不会导致某些节点不被覆盖，直到探测集合中没有这样的冗余探测为止。

随后提出了一些近似贪心算法的改进算法，在开始选择时，不是首先选择覆盖最多节点的探测，而是先挑选出被最少探测覆盖的节点，再从能覆盖到该节点的探测中选出覆盖最多节点的探测。在探测依赖矩阵中，每一列向量对应一个节点被探测经过的状态，计算每个节点对应的列向量的权值，可以得出经过每个节点的探测数，在找出被最少探测经过的节点后，可以通过计算经过它的所有探测的行向量的权值，并进行降序排列，来找出覆盖最多尚未被覆盖节点的探测，如此循环，直到所有的节点均被覆盖。

2）用于故障定位的主动探针选择技术

在故障检测阶段的工作完成后，需要对探测结果进行分析。如若检测到故障的存在，则会进行故障定位阶段的探测选择，目的是定位故障的根源。为达到该目的，需要发送合适的探测来获取更多的信息。

首先对故障检测的探测结果进行分析。若探测成功，则认为成功探测经过的所有节点均为正常节点，并将这些节点加入正常节点集合（Normal Node），当有节点之前被判定为

可疑节点时，将其从可疑节点集合中删除；若探测失败，则失败探测路径上所有之前未被判定为正常节点的节点均为可疑节点，并加入可疑节点集合（Suspicious Node）；若一条失败探测所经过的所有节点中，仅有一个节点为可疑节点，其他节点都被某些成功探测经过，那么该可疑节点即为故障节点，并被加入故障节点集合（Fault Node）。

然后，通过对故障检测阶段探测返回结果的分析，我们可以得出正常节点集合、可疑节点集合以及故障节点集合。而可疑节点集合作为状态不确定的节点集合，将成为故障定位阶段的探测目标。目前故障定位阶段的探测选择方法有两大类：预先选择探测方式和交互式选择探测方式。前者一次性选择出所有故障定位探测集合，发送到网络中并接收探测结果，预先选择的方式对网络施加固定的负荷，虽然这种方式计算过程比较简单，但是对所有的探测执行如此方式是极其低效的；交互式的探测方式是每次根据上一次探测结果自适应地选择下一个探测，这样可以有效减少所需执行探测的数量，从而得到更好的时效性和更低的额外网络负载，但计算过程往往异常复杂。

故障定位阶段的探测选择要求选择一个新的探测，该探测将要使可疑节点集合中的节点数量尽量减少。该阶段探测选择的建模也是探测依赖矩阵，和故障探测阶段的探测选择不同的是，本阶段的探测选择是从备选探测集合（未被作为探测的探测集合，在故障检测阶段表示除了故障检测集合以外的可用探测集合，在故障定位阶段表示除了故障检测集合和之前故障定位探测以外的可用探测集合）里面选取满足使可疑节点数尽量减少的探测，所以本阶段的探测必须覆盖可疑节点。

对于减少可疑节点有以下两种处理方法：方法一是，若只覆盖一个可疑节点的探测测试结果返回失败，表明该可疑节点为故障节点；方法二是，若覆盖可疑节点的探测测试结果返回成功，则表明这些可疑节点为正常节点。需要注意的是面对第二种方法时，还要考虑由于把这些可疑节点从可疑节点集合中删除，加入正常节点集合之后，之前测试集合中结果返回失败且覆盖多个可疑节点的探测可能现在只含有一个可疑节点了，需要对所有的失败的探测集合重新进行方法一的判定。技术数据的采集主要利用网络探针技术，同时结合设备MIB库变量信息、XFlow、流量探针、网元配置审计等多个数据源，多维度更全面地获取网络性能信息。

4.3 终端通信接入网运维评价体系的研究

4.3.1 综合评价的概念和基本过程

评价是指“在既定的目标下，遵从既定的原则和标准，通过特定的程序来对所选定的东西进行考核和判断”。评价的标准需要具体情况具体设定，可以偏主观，也可以偏客

观，有定性的，也有定量的，不一而足。评价是随着人类社会互动的发展而产生的，是人类认识事物的重要手段，评价活动在人类生活中处处可见，比如对员工的个人能力、工作态度等进行评价的工业绩效考核。人们对事物进行评价，其初衷往往是希望促进评价对象的发展和进步，以便能够进行更好的管理，评价运用到位，能够充分调动身边的资源，提升社会的积极性和创造性。评价的方式可分为自我总结、他评式和综合评价。

综合评价是一种整体性、全局性的评价，评价标准复杂，评价指标多样。正因为如此，许多场合都采用综合评价的方法。

综合评价同单向评价一样，必须有三大基本元素：被评价对象、评价方、评价指标。对选定好的评价问题，首先要建立综合评价基本要素，然后就要按照其既定原则对各个指标因素进行“测定”或“度量”。

4.3.2　评价指标体系建立原则

找出一个科学合理的评价指标体系是开展整个评价活动的首要任务，评价指标体系是否合乎要求将直接影响甚至是决定评价结果的可信度。对建立电力终端通信接入网的评价指标体系，必须要坚守以下几个原则：

1）客观简明性原则

客观性原则是所有原则的核心，选取指标的过程和评判重要程度时均要秉持该原则。在能够保证全面的基础上，为了指标体系的全面性不出现遗漏，指标不能过少，同时，为了指标体系不繁琐，不重叠，选取的指标也不能过多，造成评价结果出现错误、不真实，这便不能真实反映出电力终端通信接入网建设方案的优劣程度。

2）整体关联性原则

为了能全面地评价电力终端通信接入网，先要将整个系统分为若干个子系统，然后为各个子系统寻找一组指标，在选择的各个指标之间要存在一定的逻辑关联性，共同构成一个有机整体。因此指标的选取要注意层次性，自上而下，并且层层深入，从而构成一个不可分割的评价指标体系。

3）典型性原则

为了确保评价指标具有一定的代表性，应尽可能地反映出终端通信接入网的一些特征，比如经济成本、设备可靠性、投资后获得效益变化等各个方面对总体的影响。

4）全面性原则

电力终端通信接入网为一有机整体，如何全面而又贴切地建立一套评价指标体系，必须考虑全面性原则。全面而不遗漏是建立综合评价体系的基本要求。

5）可获取性原则

选择好指标后，应当对各指标在整个建设过程中的重要程度进行说明，通常数字大小往往给人最直观的感受，所以在这里应当采用量化的方法。而给出数字大小的依据来源于

真实的数据，因此，相应数据的可获取性与最终结果是密不可分的。

4.3.3 评价指标的建立过程

1. 评价影响因素分析

为了在众多建设方案中找到更符合实际且更合理的方案，对评价指标及其参数的确定应当尤为慎重，其科学性将直接影响到评价结果的准确可靠性。选取的过程要遵循前面提到的客观简明性原则、整体关联性原则、典型性原则、全面性原则和可获取性原则，力求完整准确。

2. 评价指标的确立

针对存在的问题，本章提出了一套针对终端通信接入网的评价指标体系。主要从设备、网络、经济三方面来评价终端通信接入网的建设运行状况。

1）设备

主要从设备的兼容性、可靠性以及其他性能三方面来评价。

（1）兼容性

兼容性是指不同厂家的设备相互协调工作的程度，主要反映设备网管系统的集中监控与管理能力，从具备网管功能设备比例和各厂家设备比例最大值来进行评价。

（2）可靠性

作为底层支撑网络，设备的可靠性是一个重要的评价方面。主要从丢包率、故障率、使用寿命三方面来衡量。

（3）其他特性

其他特性主要指设备自身的一些性能参数，能反映设备的承载能力、处理数据能力等。在有线接入网和无线接入网中，设备的这些特性是不一样的。

在有线网中，将CPU利用率、内存利用率、端口数量、最大MAC地址数作为评价指标。而在无线网中，将无线话音信道利用率、接收灵敏度、最大接入用户数量作为评价指标。

2）网络

（1）电网运行

电网运行主要从供电可靠性和电能质量这两方面考虑。本指标体系选取系统平均停电频率、用户平均停电频率、三相不平衡、电压波动四个指标作为评价指标。

（2）通信网运行

通信网运行主要从通信业务保障率、通信电路运行率、光缆线路运行率、无线接入性这些方面来评价。其中，无线接入性是指基站设备在通话过程中的信令信道与话务信道分配成功的情况，等于SDCCH 分配成功率与TCH 分配成功率的乘积。

3）经济

（1）成本

成本方面主要从投入成本比、运行成本比、维护成本比、故障成本比和废置成本比五个方面来考虑实际耗费成本与预估成本上限的关系。通常比值为0～1。

（2）费效比

费效比指接入网建设项目实施前后电网的静态投资变化与因电网系统服务质量提升带来效益估值的比值。

4.3.4　评价指标

1. 光纤网络评价指标体系

电力光纤专网评价体系，如表4-2所示。

表4-2　电力光纤专网评价体系

类　型	参　　数	具 体 内 容
设备概况	基本情况	单机柜最大PON口数、机框尺寸、机柜高度、机柜满配重量、整机功耗、槽位总数和用户卡槽位数
	系统容量	背板容量、单机框最大PON口数、单机柜（2m，19in）最大、PON单板数量及密度PON口数、主控板核心线速交换能力
	业务能力	上行IP业务接口能力及数量（10/100/1000M电，FE光口，GE光口，10GE光口）、上行TDM专线业务接口能力（E1/STM-1）、其他接口（GPON、时钟、级联接口）数量和类型
	设备特性	同一厂家不同型号OLT线卡可通用、用户框支持EPON/GPON线卡任意混插、升级为10G EPON方式（软件升级或其他）
设备功能	PON基本功能	OLT的MPCP发现，MPCP注册功能指标，测距功能（在线、自动和初始）；OLT对ONU的认证功能；OLT的OAM发现功能；OLT的三重搅动功能，加密后吞吐量、延时没有明显变化，达到线速加密；上行带宽分配功能（动态、静态，颗粒度）；下行流量限制功能；PON接口是否支持非工作波长，可采用外接OTDR
	二层功能	OLT本地L2交换能力及业务汇聚功能；同一PON口下实现ONU二层隔离；MAC地址学习速度（不少于1000个每秒）；MAC地址表容量（类型1≥4K，类型2≥16K）；流量控制功能；链路聚集功能；OLT的VLAN功能（支持IEEE 802.1Q 、支持4K条VLAN、支持VLAN trunk）；VLAN 优先级（支持二层QoS、802.1P）
	三层功能	三层功能（至少具有RIP/OSPF协议）
	组播功能	SCB功能验证、IGMP PROXY功能、OLT的可控组播功能、组播流静态送抵、跨VLAN/SVLAN组播、同一上行口多个组播VLAN、用户组播权限允许/禁止、用户组播预览、CDR记录以文件格式定期上传网管分析和统计CDR信息、组播带宽管理

续表

类　型	参　　数	具体内容
设备功能	DBA	DBA的最小带宽分配粒度不应大于64kbps；DBA的可配置最小带宽应该不大于512kbps；DBA的精度优于±5%
	安全功能	OLT广播/组播抑制、MAC地址数量限制、MAC地址过滤、IP地址静态绑定、IGMP协议报文的过滤与抑制
	QoS功能	OLT的上行业务流分类、排队、标记和调度；OLT的上、下行业务流限速
设备性能	组播时延性能	组播转发时延；组加入/离开时延
	TDM业务性能	E1环回功能；传输时延；抖动性能；短期/长期误码率（有≥1Gb的背景流量以验证E1的QoS保证）；E1通道带宽和承载效率（上下行承载效率）
	与ONU的性能	吞吐量（上行≥900Mbps，下行≥950Mbps）；时延（上行＜1.5ms，下行＜1ms）；过载丢包率（上行＜10%，下行＜5%）；长期丢包率（吞吐量90%时，长期丢包率为0）；是否可与其他厂家ONU互通
	系统传输能力	最大分光比
		最大传输距离和差分距离
安全要求	设备级保护	主控单元冗余备份保护；OLT电源单元的保护；PON业务板卡热插拔；配置恢复功能
	上联链路保护	以太网设备上联保护；STM-1上联链路保护
	线路保护	支持规范中保护类型；主备线路倒换时间＜50ms
维护管理	网管基本功能	网管能力（可管理的网元数和线数）不低于1000个OLT，不低于100000个ONU；与其他接入层设备统一网管平台的能力；系统软件管理；北向接口；多客户端同时操作网管系统；支持带内带外网管；数据管理
	配置管理	拓扑管理；网元管理；网元的接口参数配置；业务配置；多种设备类型统一管理；ONU设备更换自动配置下发
	故障管理	故障等级；故障信号；故障定位和屏蔽；故障清除；故障同步；告警查询和统计；支持告警智能过滤和远程通知
	安全管理	支持分权分域管理；鉴权管理；访问记录以及安全性警告提示；用户账号的自动注销（LOGOUT）；对在线维护员用户账号的维护
供电、环境和安全	供电	满配时的最大功耗，典型功耗，待机功耗；电压允许变化范围
	环境要求	温度、湿度、防尘、气压
	电气安全	绝缘电阻、设备接地要求、电磁兼容
		过压过流保护
	室外及其他恶劣环境解决方案	在室外环境和高压走廊、电气化铁路等临近范围内设备保护措施及达到指标

2. 无线专网评价指标体系

电力无线专网评价体系如表4-3所示。

表4-3　电力无线专网评价体系

类　　型	参　　数	含　　义
覆盖距离	小区接入	以基站为中心，在附近每个测试点进行多次小区搜索测试，统计小区搜索的成功率，记录相应的RSRP值，并记录UE到基站的距离
	随机接入	以基站为中心，在不同方向上每个测试点进行多次随机接入测试，统计随机接入的成功率，记录相应的RSRP值，并记录UE到基站的距离
	业务覆盖距离	对基站测试业务的覆盖距离。UE选择远离基站不同距离的位置，建立小区，以最低码率的QPSK调制方式做数传业务，并保持一段时间，记录该位置的RSTP、BLER和系统吞吐量，直到BLER达到10%，测得的UE能正常做业务的最远距离，就是业务覆盖的最大距离
吞吐量	吞吐量	测试不同调制编码方式下系统传输速率数据。从UE测试发送2Mb的数据包，在模拟主站侧统计收到的数据包的速率，统计10min，记录平均值，作为基站的最大传输速率
容量	网络容量	核心网处理能力指标，即可支持一定质量通信终端数目
	基站处理能力	基站在支持一定数量终端通信时CPU利用率及所占内存
	空口容量	系统空口支持的最大用户数
同频性能	相邻小区同频组网RSRP值的相互影响	
抗干扰性能	带外干扰对系统通信性能的影响	
业务承载能力	系统稳定性	系统无故障运行时长
	信道传输时延	不同频点信道传输时延
	信道连通性	信道连通时长
	信道误块率	信道通信误码率性能

3. 中压载波评价指标体系

中压载波通信设备的功能和评价指标主要包括载波工作频段、发送功率和工作温度范围等，详细见表 4-4。

表4-4　中压载波通信设备技术参数和评价指标

名　　称	项　　目	标准参数值
载波通信设备通用评价指标	载波频段	20～500kHz 可自动动态调整
	数据接口	RS-232或RS-485
	串口传输率	300bps、600bps、1200bps、2400bps、4800bps、9600bps、19.2kbps、38.4kbps可设
	传输误码率	$<10^{-5}$
	适用电压等级	35kV、10kV
	最大载波发送功率	5W
	接收灵敏度	<-60dBm
	接收信噪比	≥-3dB
	工作温度范围	-40℃～+65℃
	通信协议	支持主从通信协议、透明数据传输、101规约

续表

名　　称	项　　目	标准参数值
载波通信设备通用评价指标	回波损耗	≥25dB
	输出阻抗	75
	散热	无风扇散热
	应用案例	提供不少于3处典型案例
	设备应用	提供不少于500台现场运行设备证明
主载波设备评价指标	工作电源	AC220V/DC220V/DC±48V/DC24V
	外形结构	19in宽度，2U或4U高度
	网管接口	必须具备独立的网管接口，以监测所管辖逻辑网络的载波设备的运行状态；具有支持综合网管的北向接口
从波设备评价指标	工作电源	AC220V/DC220V/DC±48V/DC24V
	外形结构	小型化设计，外形≤300mm×300mm×100mm
	中继	既可作普通从载波设备也可同时作为中继载波设备
	稳定性	单台从载波出现故障时，故障范围只能局限于该故障节点，不能扩大影响到其他节点正常通信
注入式电感耦合器评价指标	载波频段	20～500kHz
	线路侧标称阻抗	75Ω
	传输衰耗	＜4.5dB
	额定功率	＞100W
	工作环境温度	-40℃～+65℃
	单脉冲电流承受力	30kA
卡接式电感耦合器评价指标	载波频段	20～500kHz
	线路侧标称阻抗	75 Ω
	传输衰耗	＜8.5dB
	额定功率	＞100W
	工作环境温度	-40℃～+65℃
	工作环境	可浸泡在水中工作
	安装	不停电安装
一体化电容耦合器评价指标	安装环境	适合室内外环境安装
	载波频段	20～500kHz
	线路侧标称阻抗	75 Ω
	传输衰耗	＜4.5dB
	额定功率	＞100W
	工作环境温度	-40℃～ +65℃
载波通信管理机评价指标	支持以太接口到串口镜像	可配置不少于4个串口镜像
	对主载波接口	RS-232或RS-485
	上联接口	100Mbps以太网
	网络管理功能	对载波网络进行网管、故障定位，传输性能监视

续表

名　称	项　目	标准参数值
载波通信管理机评价指标	供电电源	AC220V/DC220V/DC48V/DC24V
	可管理的主载波数量	≥10台
	外形结构	19in宽度，1U或2U高度
	散热	无风扇散热技术
	工作温度	-10℃～+65℃

4. 无线公网评价指标体系

无线公网数据接入评价指标如表4-5所示。

表4-5　无线公网数据接入评价指标

指标名称	含　义
应用层平均速率	应用层传送文件数据量（kbps）/实际传送时间
数据掉线比	应用层传送文件数据总量/掉线次数
掉线率	掉线次数/链路建立成功次数，1min无数据或PDP去激活计为掉线
吞吐量	定义为应用层的吞吐量，该吞吐量又分为上行吞吐量和下行吞吐量
接入时长	接入时长定义为从终端开始拨号到建立PPP（点对点协议） 连接的时间
时延	分组从发出起，到目的主机收到该分组的这段等待时间。用户希望网络的反应速度快，时延小。例如 CDMA 2000 的总时延包括天线业务信道建立时延、链路层协议初始化时延、传输时延、服务器响应时延等
从休眠到激活状态的时间	定义为当终端进入休眠状态后，无论从终端侧还是网络侧发起响应，终端从休眠状态到激活状态的时间

5. 整体网络评价指标体系

终端通信统一接入网评估指标除光纤专网、无线专网和无线公网固有指标外，重点涉及融合网络性能。整体网络评价指标如表4-6所示。

表4-6　整体网络评价指标

类　型	指　标	含　义
业务开通指标	业务开通时长	指从接到业务需求通知开始到能够正常提供通信业务服务的历时时长
	业务开通及时率	为在规定电路开通时间内开通的业务总数与要求开通业务的比例
业务可用率指标	数据业务可用率	数据业务可用率=1-∑（中断的数据业务带宽数×不可用时长）（分钟）/全部数据业务带宽总数×运行总时长（分钟）
光纤与无线融合组网	OLT上行端口入流量平均带宽利用率	OLT上行端口入流量平均带宽利用率＝OLT上行端口全天总接收比特数/（OLT上行端口最大带宽×24×60×60），上行端口入流量包括流入融合网络中无线终端流量
	OLT上行端口出流量平均带宽利用率	OLT上行端口出流量平均带宽利用率＝OLT上行端口全天总发送比特数/（OLT上行端口最大带宽×24×60×60），上行端口出流量包括流出融合网络中无线终端流量

续表

类　　型	指　　标	含　　义
光纤与无线融合组网	OLT上行端口入流量峰值带宽利用率	OLT上行端口峰值入流量/OLT上行端口最大带宽。流量包括融合网络中无线终端及有线终端的通信流量
	OLT上行端口出流量峰值带宽利用率	OLT上行端口峰值出流量/OLT上行端口最大带宽。流量包括融合网络中无线终端及有线终端的通信流量
	任一ONU到数据网时延	指从城域数据网ping相应OLT下挂ONU的管理地址（或用户地址）得到的时延
	任一无线终端到数据网时延	指从城域数据网ping相应OLT→ONU→无线终端的管理地址得到的时延
	任一ONU到数据网丢包率	基于城域数据网 ping 相应OLT下挂ONU的管理地址（或用户地址）得到的丢包率
	任一无线终端到数据网丢包率	基于城域数据网 ping 相应OLT→ONU→无线终端的管理地址（或用户地址）得到的丢包率
无线公网指标	通信可靠性	公网通信终端C、SIM卡损坏率
	终端掉线率	终端通信中断超过1min的比率
	运维平均时长	通信发生中断后修复平均时长
	网管信息分享程度	公网网管信息接入到电力终端通信网接入网管的信息量
	不同制式终端接入能力	不同运营商终端统一接入能力
成本	单终端平均成本	统一组网后，单终端平均组网成本
	单终端平均运维成本	统一运维人员和运维流程后，单终端平均运维成本

6. 运维评价指标体系

运维评价指标如表4-7所示。

表4-7　运维评价指标

项　　目		内　　容	要　　求
资源配备	人员数量		按要求配置维护和工程人员
	人员变更		年变动率每组不超过1人，需事先申请并得到批准
	人员资质		学历、上岗证和专业证件符合要求
	车辆与仪表		车辆和仪表配备符合要求
月度计划与完成情况	工作计划、检测计划、计划变更	上报及时性	每月定期上报计划
		准确完整性	与实际完成情况相符
		完成进度	按进度完成巡检工作，与计划不符的要详细说明
		计划变更	提前2天书面申请
	检测报告质量		检测方法正确，结果反映设备和网络质量真实情况
报表	月、季度、半年度报表		
	工程资料和基础数据库	及时性	按分公司要求定期上报资源数据库和固定资产更新等资料，按工程工作要求上报竣工资料
		准确完整性	完整并与实际情况相符

续表

项 目		内 容	要 求
整改情况	异常情况报告单	上报情况	对于无法处理的问题要立即上报，并跟踪处理结果
		整改及时性	在工单规定的时限内
		整改质量	符合整改质量要求
		记录与回单	记录详尽、真实，整改后2天内回单
		耗材	耗材质量符合要求，记录情况（如型号、规格和数量等）与实际相符
	整改通知单	整改及时性	在工单规定的时限内
		整改质量	符合整改质量要求
		记录与回单	记录详尽、真实，整改后2天内回单
		耗材	耗材质量符合要求，记录情况（如型号、规格和数量等）与实际相符
故障投诉处理和工程工作	故障、投诉处理通知单/工程工作工单	工作及时性	工单处理及时率（包括故障效应不及时、处理不及时等）
		工作质量	维护工作：判断准确，故障不反复；工程工作：施工规范，质量符合要求
		记录与回单	记录详尽、真实，处理后1天内回单
		故障件返还	2天内
		耗材	耗材质量符合要求，记录情况（如型号、规格和数量等）与实际相符
随工工作	随工工作	随工及时性	及时随工
		随工质量	质量符合工程规范和维护要求
		随工纪律	随工人员认真遵守随工制度
		记录与回单	记录详尽、真实，完工后2天内回单
服务态度	合作配合		服务规范、热情，态度好
	用户投诉		客户无意见
	分公司临时布置工作		按时、按质完成任务
	联络畅通		24小时值班电话必须联络畅通
安全情况	安全性		按照维护规范和安全生产规范开展运维工作，保证无安全事故发生
	操作规范性		操作规范
	严重违约		严格遵守协议要求
	上报		发现安全隐患或发生安全问题要立即上报

4.3.5 终端通信接入网运维评价方法介绍

1. 层次分析法

1）层次分析法概述

层次分析法（Analytic Hierarchy Process，AHP）是将与既定目标密切相关的全部关键

因素汇总起来，根据一定的原则将其分解为目标层、准则层、方案层等，层次数目可以根据具体项目情况而定，之后依据划分好的层次，对各个因素进行定量和定性分析，为决策者做出决定提供科学可靠的参考标准。

2）层次分析法基本步骤

（1）建立系统的层次结构模型

想要对一个难以着手的问题开展分析，具体做法是：首先要确定好需要分析的问题，找准主题并进行深入分析，以此为基础确定出评价目标；之后根据确定好的目标，构造出符合条件的评价指标体系，然后据此评价体系，按其中基本关系从上而下地分解为几个层次级别。该层级结构需要遵循以下几个规则：低一级的指标是相对应的高一级指标的子指标，如果产生变化则能对上级指标产生影响；而上一级指标又可控制下一级别的指标；同级别的各指标保持相互独立。

层次结构的划分如图4-4所示。

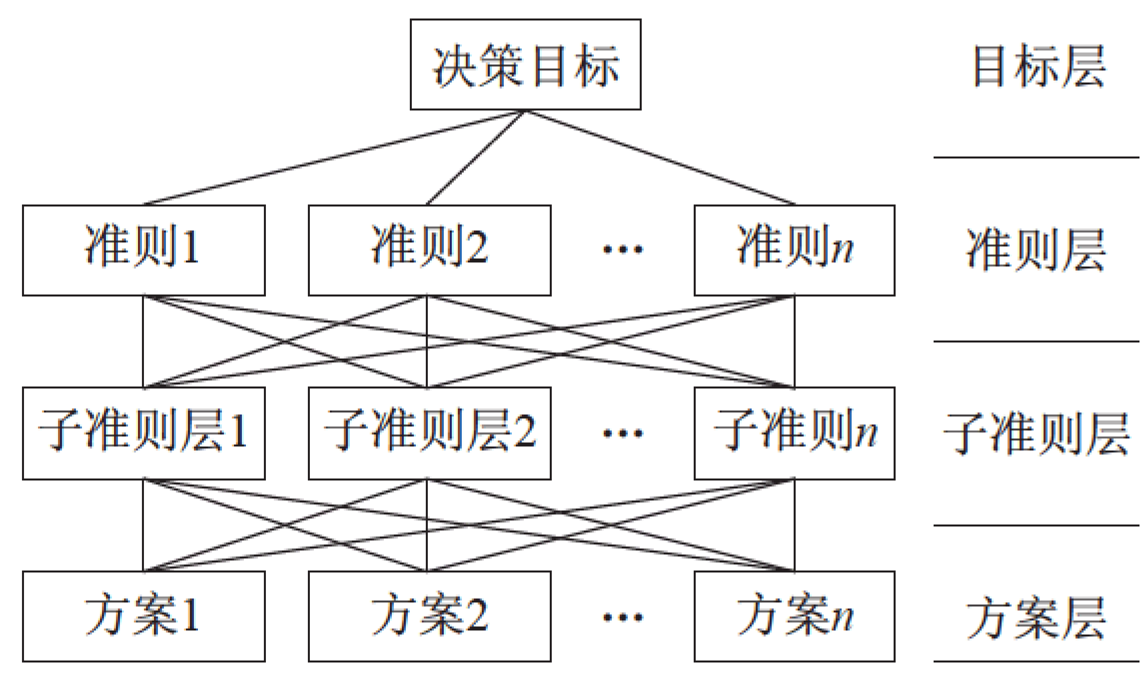


图4-4　层次结构划分示意图

层数的确定需要具体问题具体分析，简单一点的问题就设置全面一点，这样可以使之更明确，复杂的问题就在保证全面的前提下简洁一点。构建层次模型时尽量确保每层指标数目不超过9个，以免给两两比较矩阵的构造带来困难。

（2）构造两两比较矩阵

从第二层——准则层开始，需要比较同一层次中各个指标关于上一层次同一指标的相对重要性，这里的相对重要性应当基于同一个标准，这个标准则来自于将其划分为同一层次的依据；然后把相同层各指标两两对比，判断出指标重要程度的大小，如此一来就将重要程度转化为可以度量计算的数值，构成一个判断矩阵。从上至下，将各层的每个指标的相对重要性都要比较出来，具体的量化方法采用的是Satty等人提出的1-9标度法，如表4-8所示。

表4-8　1-9标度法

尺度	1	2	3	4	5	6	7	8	9
指标间相对重要程度	相同		稍强		强		明显强		绝对强

假设下层指标为N_1，N_2，N_3，…，N_n，相对应的上层目标指标为M，则其判断矩阵如

表4-9所示。

表4-9　判断矩阵

M	N_1	N_2	…	N_n
N_1	a_{11}	a_{12}	…	a_{1n}
N_2	a_{21}	a_{22}	…	a_{2n}
⋮	⋮	⋮	⋮	⋮
N_n	a_{n1}	a_{n2}	…	a_{nn}

其中a_{ij}表示对于上一层指标M来说，其下一层子指标N_i对子指标N_j的相对重要性的数值表示。

判断矩阵需要满足以下性质：

ⓐ $a_{ij}>0$；

ⓑ $a_{ji}=1/a_{ij}$；

ⓒ $a_{ii}=1$。

由上面结论能够得到，当一个判断矩阵满足以上3个性质的时候，该判断矩阵就被称为一致性矩阵，一致矩阵说明对各个指标相对重要性的判断是连贯的，是合理的。然而在实际操作中，大部分情况下生成的判断矩阵都不是一致性矩阵，因此，需要确定出不一致的允许范围。

（3）计算各指标相对权重并进行一致性检验

相对权重指的是只在同一个目的基础下，所选出的各项指标在这个目的实现的过程中占有的重要程度比重。要想计算出相应的数值，首先要计算出相应的判断矩阵的最大特征根及其对应的特征向量。最大特征向量的归一化结果就是其相对权重的结果。计算出相对权重结果后，还得对其进行一致性检验，只有通过了一致性检验，其结果方能采用，若不通过，还需回到上一个步骤构造新的判断矩阵。

因为在通常情况下，判断矩阵不是一致性矩阵，那么只要不一致在允许的范围内，就接受其结果，也就是说满足大体上的一致性即可。判断一个判断矩阵的一致性，其步骤如下：

步骤1　计算出指标一致性CI。CI表达式如下：

$$CI=\frac{\lambda-n}{n-1}$$

其中λ为矩阵的最大特征值，n表示矩阵的维数。CI应该越小越好，CI=0说明该矩阵为一致矩阵，CI与0偏差越大说明不一致现象越严重。

步骤2　需要通过检测CI的合理性来确定是否接受所得到的结果，这时需要引入平均随机一致性指标RI。RI的值可以查表获得，表4-10给出了1到9阶的RI的值。

表4-10　1-9阶RI值

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

步骤3　计算一致性比率CR并进行判断：

$$CR = \frac{CI}{RI}$$

当$CR<0.1$时，认为判断矩阵的一致性在可接受的范围内，接受其判断结果；若$CR>0.1$，则认为判断矩阵一致性不符合要求，需要对判断矩阵进行修正。

（4）计算指标整体权重并做整体一致性检验

在上一个步骤中确定了准则层和方案层各个指标的相对权重，下一步就需要将各指标的整体权重计算出来。整体权重代表该指标在整个方案中所占的分量，其计算是采用自顶向下的方法，一层一层地将权重系数相乘得到结果。

同指标权向量一样，也需要对整体权重做整体一致性检验。如果检验结果在允许范围内，就可以使用计算出来的整体权重结果来对问题进行求解或决策；如果检验结果超出允许范围，就需要重新考虑改变模型结构或对那些一致性结果比较大的判断矩阵进行重新构造。

3）层次分析法优点

层次分析法可以把所研究的问题层层细分，而细分后的各指标又紧密相关，组成一个有机的整体，从而将一个复杂的问题层级分解后简单化。在确定好各个部分的指标后，就能够通过专家意见进行综合判断，进而计算出各指标所占的权重，为问题的解决做出最好的决策。鉴于层次分析法的特点，可以看出层次分析法具有以下几个优点：

① 建立了所有要素（包括非量化与量化）的层级，清楚呈现各层、各准则与各要素的关系。这使得所分析的问题变得有层次、有条理，同时也突出了各分割部分的重点。

② 将问题数量化，便于计算。在将问题划分好层次，选定好指标后，可以计算出各指标的权重，使人们看到数据后对问题的重点一目了然，而且还有针对指标判断矩阵的一致性检验，使得到的数据具有科学性，可信度较高。

③ 可操作性强。计算矩阵向量权值时，除了利用传统的数学方法计算之外，还可以利用计算机软件比如功能强大的MATLAB，通过MATLAB软件编程来处理数据，降低工作的复杂性和难度。

因此层次分析法是一种强有力的分析方法，对多元素、多原则、多方法的综合评价及趋势预测能发挥很大作用。而且该方法提出的“目标层—准则层—方案层”的层次划分，为解决难以定量描述问题给出了办法。

2. 模糊综合评价法

模糊综合评价法以其简便的特点广泛应用于业务质量，是对网络的性能等方面的评价。其步骤主要是：

（1）确定评价指标集$U=\{u_1, u_2, \cdots, u_n\}$

将不同量纲的指标，通过适当变换，转化为无量纲的标准化指标，这一过程称为指标

的无量纲化处理，也就是定量指标量化的过程。x_{ij}为x_i的观测值，归一化公式为

$$x_{ij}^{*}=\frac{x_{ij}}{\sum_{i=1}^{n}x_{ij}}$$

（2）确定影响因素权重

确定对评价因素集中元素的权重$A=\{w_1, w_2, \cdots, w_n\}$是评价的核心。

（3）确定评语集

评语集$V=(v_1, v_2, \cdots, v_M)$是对评判对象可能做出的各种评价结果所组成的集合。

（4）确定隶属关系，建立模糊关系矩阵

通过寻找因素集中元素与评语集中元素的隶属关系，建立隶属函数，确定隶属度。单个因素构成的评判向量$RI=(RI_1, RI_2, \cdots, RI_M)$，可知所有单因素的模糊向量构成因素模糊评判矩阵：

$$\boldsymbol{R}=\begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ r_{31} & r_{32} & \cdots & r_{3m} \end{bmatrix}$$

隶属度的确定：简单方法是等级比重法。这种方法要求评价者通过若干个指标对被评价对象属于哪个等级做出判断，然后把根据第i个指标而将评价对象判断为第j个等级的人数与全部评价者人数的比值作为RI_j。

（5）确定模糊综价指标

将单因模糊评判矩阵与各个因素的权重集进行模糊运算，即得到模糊综价指标

$$\boldsymbol{B}=\boldsymbol{AR}=\begin{bmatrix} w_1 & w_2 & \cdots & w_m \end{bmatrix}\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ r_{31} & r_{32} & \cdots & r_{3m} \end{bmatrix}=\begin{bmatrix} b_1 & b_2 & \cdots & b_m \end{bmatrix}$$

（6）评价结果

等级参数评判法：设法将模糊子集B转化为一个分值，根据这个分值来划级或排序，因此需要给出一组关于等级的参数值，即等级参数向量（$w_1, w_2, \cdots, w_M$）。确定出等级划分的分数线标准之后即可根据各等级的总分比较最优值来断定业务服务质量所属等级。

$$S=BW=\sum_{j=1}^{m}B_jW_j$$

3. 数据包络分析法

数据包络分析法能够对各个指标的相对有效性做出评价，找出各个指标的弱点，且无

须任何权重假设，每一输入输出的权重不是根据评价者的主观判断来确定，而是根据实际数据求得最优权重，从而排除了人为因素带来的偏差，具有很强的客观性。

（1）确定评价指标集和评价等级集

设$A=\{A_1, A_2, \cdots, A_n\}$为对象集，$B=\{B_1, B_2, \cdots, B_M\}$为评价指标集，$M$为评价指标的个数，$n$为待评价业务数目；$C=\{C_1, C_2, \cdots, C_k\}$为评价等级集，$k$为评价等级的个数，通常为3～5。

（2）构造评价指标的隶属度矩阵

针对每一个评价指标B_j（j=1, 2, …, M），构造一个模糊关系矩阵$\boldsymbol{R}_j$（j=1, 2, …, M），$\boldsymbol{R}_j$为$\boldsymbol{B}_j$的隶属度矩阵。首先对第i个评价对象A_i作单对象评判，评价指标B_j能被评价为等级C_h（h=1, 2, …, k）的隶属度为RI_{jh}，这样就得到了评价对象A_i的单对象评判向量$\boldsymbol{RI}_j$=（RI_{j1}, RI_{j2}, …, RI_{jk}）（i=1, 2, …, n；j=1, 2, …, M），则n个A_i的属于统一等级j的评判向量就构成一个新的隶属度矩阵$\boldsymbol{R}_j$：

$$\boldsymbol{R}_j=\begin{bmatrix} r_{1j} \\ r_{2j} \\ \vdots \\ r_{mj} \end{bmatrix}=\begin{bmatrix} r_{1j_1} & \cdots & r_{1j_k} \\ \vdots & & \vdots \\ r_{mj_1} & \cdots & r_{3m} \end{bmatrix}$$

（3）确定最优目标函数值矩阵

它是针对每一个决策单位建立对其最有利的数学规划模型，通过解其最优解来判断其有效性。这里选择DEA模型作为采用的模型。

$$\boldsymbol{H}=(H_1,H_2,\cdots,H_n)=(h_{ij})=\begin{bmatrix} h_{11} & \cdots & h_{1n} \\ \vdots & & \vdots \\ h_{m1} & \cdots & h_{mn} \end{bmatrix}$$

（4）综合评价结果的确定

将第i个对象A_i（i=1, 2, …, n）与针对所有评价指标的最优目标函数值h_{ij}相乘，其积g_i可作为该综合评价结果：

$$g_i=\prod_{j=1}^{n} h_{ij}, i=1,2,\cdots,m$$

4.3.6 终端通信接入网运维评价方案确定及算例分析

1. 评价方法选择

（1）确定各级指标的权重

首先确定各级指标的权重。

① 利用1—9标度法（见表4-11），采用专家判断，对各级指标进行两两重要度比较，确定各判断矩阵。

表4-11　1—9标度法

等　级	语言描述程度	含　义
1	同等	指标a和指标b同等重要
3	稍微	指标a比指标b稍微重要
5	明显	指标a比指标b明显重要
7	强烈	指标a比指标b强烈重要
9	极端	指标a比指标b极端重要

② 检验判断矩阵一致性。

对各指标进行归一化：

$$x_j(j)=\begin{cases}\dfrac{x_i(j)-\min\limits_i x_i(j)}{\max\limits_i x_i(j)-\min\limits_i x_i(j)} & \text{越大越优型}\\[2ex] \dfrac{\max\limits_i x_i(j)-x_i(j)}{\max\limits_i x_i(j)-\min\limits_i x_i(j)} & \text{越小越优型}\end{cases} \tag{4-1}$$

其中，i表示第i个序列，j表示第j个指标。

（2）计算关联度

利用灰色关联分析计算各待评价序列与参考序列的关联程度。

$$\xi(x_0(k),x_i(k))=\frac{m+\varepsilon M}{V_{0i}(k)+\varepsilon M} \tag{4-2}$$

其中，$V_{0i}(k)=|x_0(k)-x_i(k)|$，为各个序列值与参考序列的绝对差。$m=\min_i \min_k V_{0i}(k)$，表示所有待评价序列在第$i$个指标序列中的最小值。$M=\max_i \max_k V_{0i}(k)$，表示所有待评价序列在第$i$个指标序列中的最大值。$\varepsilon$为分辨系数，一般取值0.5。

（3）确定评价结果

进行关联度排序，确定评价结果。

$$\gamma(x_0,x_i)=\sum_{k=1}^{N}w(k)\xi(x_0(k),x_i(k)) \tag{4-3}$$

（4）多级评价

利用下级指标关于上一级指标的关联度与上一级指标的权重进行加权求和。

2. 算例分析

本例列举3个地区的终端通信接入网作为算例参考，待评价网络包含有线接入网和无线接入网，以有线/无线覆盖面积所占总面积之比作为其权重。

各指标权重以及待评价网络具体指标值如表4-12所示。

表4-12　待评价网络具体指标值

一级指标	二级指标	三级指标		参考值	网络1	网络2	网络3
设备0.4094	兼容性0.3714	各厂家设备比例最大值0.5791		1	0.6	0.4	0.5
		具备网管功能设备比例 0.4209		1	0.85	0.9	0.76
	可靠性0.3429	丢包率0.3335		0	0.01	0.03	0.05
		故障率0.3214		0	0.05	0.03	0.01
		使用寿命0.3451		0	8.6	5.3	7.3
	其他特性0.2857	有线0.78	CPU利用率0.5739	0.35	0.22	0.31	0.51
			内存利用率0.1600	0.6	0.34	0.45	0.25
			端口数量0.1913	48	12	24	16
			最大Mac地址数量0.0748	8000	4000	3000	6000
		无线0.22	无线话音信道利用率0.3451	0.7	0.35	0.37	0.5
			接收灵敏度（dBm）0.3335	−85	−76	−70	−81
			最大接入用户数量0.3214	80	78	48	56
网络0.3018	电网运行0.5813	系统平均停电频率0.6426		0	0.024	0.04	0.035
		系统平均停电时间0.0480		0	30	26	23
		三相不平衡0.2084		0	1%	1.5%	0.9%
		电压波动0.1010		0	1.3%	2.1%	1.6%
	通信网运行0.4187	通信业务保障率0.388		1	0.9	0.86	0.94
		通信电路运行率0.322		1	0.88	0.79	0.84
		有线0.78	光缆线路运行率0.290	1	0.87	0.79	0.85
		无线0.22	无线接入性0.290	1	0.81	0.78	0.86
经济0.288	成本	投入成本比0.375		1	0.7	0.55	0.78
		运行成本比0.263		1	0.87	0.76	0.96
		维护成本比0.055		1	0.69	0.97	0.56
		故障成本比0.099		1	0.88	0.69	0.91
		废置成本比0.110		1	0.79	0.87	0.79
	费效比	年均费效比1		1	0.89	0.72	0.83

对原始数据矩阵无量纲化，由式（4-2）可计算出三级指标的关联系数矩阵。

$$\xi_{01}=\begin{pmatrix} 1 & 0.78 & 0.88 \\ 0.82 & 1 & 0.61 \end{pmatrix} \qquad \gamma_{01}=(0.9242 \quad 0.8726 \quad 0.7664)$$

$$\xi_{02}=\begin{pmatrix} 1 & 0.64 & 0.47 \\ 0.47 & 0.64 & 1 \\ 0.75 & 1 & 0.83 \end{pmatrix} \qquad \gamma_{02}=(0.7434 \quad 0.7642 \quad 0.7646)$$

$$\xi_{03}=\begin{pmatrix} 0.57 & 1 & 0.50 \\ 0.79 & 1 & 0.65 \\ 0.78 & 1 & 0.84 \\ 0.69 & 0.6 & 1 \end{pmatrix} \quad \gamma_{03}=(0.6543 \quad 0.9701 \quad 0.6264)$$

$$\xi_{04}=\begin{pmatrix} 0.71 & 0.74 & 1 \\ 0.7 & 0.51 & 1 \\ 1 & 0.37 & 0.45 \end{pmatrix} \quad \gamma_{04}=(0.7999 \quad 0.5444 \quad 0.8232)$$

γ_{03}和γ_{04}分别表示有线和无线设备的特性，根据其权重对其进行加权运算，可得到待评价网络的设备其他特性的灰色关联度矩阵为：

$$\gamma_{034}=(0.6863 \quad 0.8764 \quad 0.6697)$$

$$\xi_{05}=\begin{pmatrix} 1 & 0.73 & 0.80 \\ 0.85 & 0.93 & 1 \\ 0.94 & 0.73 & 1 \\ 1 & 0.75 & 0.89 \end{pmatrix} \quad \gamma_{05}=(0.9803 \quad 0.7416 \quad 0.8604)$$

$$\xi_{06}=\begin{pmatrix} 0.77 & 0.62 & 1 \\ 1 & 0.71 & 0.88 \\ 1 & 0.75 & 0.93 \\ 0.84 & 0.76 & 1 \end{pmatrix} \quad \gamma_{06}=(0.9005 \quad 0.6873 \quad 0.9455)$$

$$\xi_{07}=\begin{pmatrix} 0.85 & 0.66 & 1 \\ 0.64 & 0.45 & 1 \\ 0.48 & 1 & 0.38 \\ 0.89 & 0.53 & 1 \\ 0.75 & 1 & 0.75 \end{pmatrix} \quad \gamma_{07}=(0.7727 \quad 0.6381 \quad 0.9393)$$

$$\xi_{08}=(1 \quad 0.59 \quad 0.80) \quad \gamma_{08}=(1 \quad 0.59 \quad 0.80)$$

由以上关联度矩阵可以看出，在设备兼容性方面，网络1最优，网络2其次，网络3最差；在设备可靠性方面，网络3最优，网络2其次，网络1最差；在设备的其他特性方面，网络2最优，网络1其次，网络3最差；在电网运行方面，网络1最优，网络3其次，网络2最差；在通信网运行方面，网络3最优，网络1其次，网络2最差；在经济成本方面，网络3最优，网络1其次，网络2最差；在费效比方面，网络1最优，网络3其次，网络2最差。

通过二级指标权重与三级指标的关联度矩阵的加权运算，可得到各二级指标的关联度矩阵，如下所示。

$$\boldsymbol{\psi}_{01}=(0.7942\quad 0.8365\quad 0.7382)$$

$$\boldsymbol{\psi}_{02}=(0.9469\quad 0.7189\quad 0.8960)$$

$$\boldsymbol{\psi}_{03}=(0.8878\quad 0.6138\quad 0.8688)$$

由以上三式可知，在接入网设备方面，网络2最优，网络1其次，网络3最差；在网络运行方面，网络1最优，网络3其次，网络2最差；在经济性方面，网络1最优，网络3其次，网络2最差。

通过一级指标的权重与二级指标的关联度矩阵的加权运算，可得到总评价目标的关联度矩阵，如下所示。

$$\boldsymbol{\varphi}=(0.8673\quad 0.7367\quad 0.8235)$$

因此，该3个待评价网络的排序为网络1＞网络3＞网络2。

4.4 总　　结

终端通信接入网的规划建设是全面实现配电和用电环节信息化、自动化和互动化的重要支撑和保障，对终端通信接入网的现状、需求和政策进行分析和研究，将为智能电网配用电环节的建设、生产、运行、维护等方面起到指导和保障作用。终端通信接入网的发展是智能电网配用电环节建设的坚实基础；是推动电力光纤到户服务“三网融合”业务的有力保障；是加快清洁能源接入、倡导节能减排的有效手段；是实现坚强智能电网，建设“一强三优”现代化企业的重要体现。终端通信接入网主要覆盖配电网开关站、配电室、环网柜、柱上开关、配电变压器、分布式能源站点、配电线路等，主要承载配电自动化接入层、用电信息采集系统远程信道、智能小区上联通道的信息通信业务。

结合电力终端通信接入网的需求及所存在的问题，本章选取了层次分析法和灰色关联度分析法相结合的评价方法进行电力终端通信接入网的评估，并结合专家的意见对各个层次的指标建立判断矩阵，根据判断矩阵找出最大特征值，并对相应的特征向量归一化计算，得出各个指标相对权重，然后又通过相对权重计算出组合权重，最后结合算例分析，示范如何运用本评估方法找到最佳的建设方案。此处所建立的评价指标体系是相对全面的，涵盖了经济性因素和技术性因素，而且运用层次分析法和灰色关联度分析法相结合的方法对电力终端通信接入网进行评价，所得到的结果是客观科学的，为以后的终端通信接入网建设项目提供了参考依据。随着终端通信接入网的不断发展，对其进行的评价工作也应该随其发展的速度不断更新，为建设一个更好的终端通信接入网不断努力，并且做出贡献。

第5章

电力终端通信接入网规划



5.1 终端通信接入网业务分析

5.1.1 生产类业务

1）配电自动化系统

单个终端接入速率要求为光纤专网≥19.2kbps，其他方式≥2.4kbps。配电自动化信息“二遥”业务包括整点数据上传、实时召唤及越限信息实时上传业务。整点召唤业务频率可根据需要设置，采集时间间隔为1min～1h。不同通信方式的遥测、遥信时延要求不同，遥测要求光纤＜2s，载波通信＜30s，无线通信＜60s；遥信要求光纤＜2s，载波通信＜3s，无线通信＜30s；所有通信方式的遥控要求相同，遥控要求≤6s。

三遥信息属于生产控制业务，对于信息安全性要求高，只能采用专网通信方式传输；二遥业务属于生产业务，但无控制信号传输。为降低通道建设成本，对于信息安全要求略低于三遥业务的，可以采用公网无线虚拟专网技术传输。

2）10kV线路保护

10kV线路保护指采用专用光纤纤芯进行双向传输10kV线路保护信号，为专用光纤方式。

3）分布式电源

分布式电源通信内容包括配电自动化、营销业务，有电能质量监测、分布式电源监控（含调度远动）、计量信息三种类型。10kV分布式电源终端单点接入的流量是42.3kbps，380/220V分布式电源终端单点接入的流量是1.05kbps。遥测、遥信要求相同，光纤通信＜3s，载波通信＜30s，无线通信＜60s；遥控要求光纤通信≤10s，载波通信≤60s。孤岛监测和故障隔离时间要求远程方式≤300s，本地方式≤3s。

10kV、35kV分布式电源同时具有自动化业务和营销业务（电量计量），对于通道的信息安全性、可靠性、时延要求高，需要专网通道传输。380/220V分布式电源，只有用电信息采集和计量业务需求，对信息安全性和可靠性的要求等同于用电信息采集信息，专网可以覆盖的情况下可以采用专网传输，无专网覆盖的区域，可以采用公网无线通信技术传输。

5.1.2 管理类业务

1）用电信息采集系统

用电信息采集系统通信内容主要为电压、电流、有功功率、无功功率、用户电量、关口电量等采集信息及费率控制信息。数据流向为电表终端—采集终端—用电信息采集主站，通信传输速率为9.6～115.2kbps，采集终端每15min抄收一次电表信息，采集终端每天上传一次数据给主站。遥控操作响应时间小于5s，数据召测响应时间小于15s。

该类业务对于实时性、信息安全性的要求低于生产业务，光纤专网、无线专网覆盖的区域应采用专网通信技术传输，无专网覆盖的区域采用无线公网传输。

2）380V分布式电源

380V分布式电源只有用电信息采集和计量业务需求，对信息安全性和可靠性的要求等同于用电信息采集信息，专网可以覆盖的情况下可以采用专网传输，无专网覆盖的区域可以采用公网无线通信技术传输。

3）电动汽车充电站（桩）

目前，电动汽车充电站（桩）接入类型包括充电桩以及集中充电站，集中充电站由数十至数百个充电桩组成。业务数据流向：充电桩通信终端—省公司前置服务器—车联网平台；单个充电桩传输速率要求约为4kbps。系统对采集类数据的时延要求小于5s，数据召测时间间隔为5min。

该类业务属于用电信息采集类业务，对于传输通道的实时性、信息安全性低于生产类业务，专网覆盖的区域应采用专网传输，无专网覆盖的区域，可采用无线公网通信技术传输。

4）移动巡检

语音业务通信传输速率为8～64kbps，视频业务为384kbps～2Mbps，数据业务为64kbps～2Mbps，语音和视频类业务对时延和可靠性要求较高。

该类业务属于用移动大颗粒管理业务，要求采用移动通信手段传输，对于通道带宽、时延要求较高，信息安全性低于生产类业务，专网覆盖的区域应采用专网传输，无专网覆盖的区域可采用无线公网通信技术传输。

5）配网抢修

传输速率需求约为4Mbps，时延要求为百毫秒级，对通道的要求同上。

6）配电设备/环境状态监测

配电设备/环境状态监测目前出于试点研究阶段，对带宽要求较低，实时性要求不高，单个接入点的速率需求约为几千比特每秒，传输时延为秒级。未来规模化部署时，配电监测点数量庞大，监测位置分布分散。该类业务对信息安全性能要求低于生产业务，在无线专网覆盖的区域，应采用无线专网传输，没有无线专网的区域，应采用无线公网技术传输。

7）变电站、分布式电源电能质量监测

变电站、分布式电源电能质量检测业务，带宽要求高于1Mbps，属于内网传输信息，需要采用专网通信方式传输。

8）输变电状态监测

输变电状态监测对实时性要求较高，传输时延小于1s，单个接入点的带宽需求约为2Mbps。对于信息安全性要求低于生产业务的，无线专网覆盖的区域采用专网传输，无无线专网的区域，应采用无线公网传输。

9）机器人巡检

该类业务属于移动业务，数据包括图像、设备诊断等信息，传输速率要求大于4Mbps，对时延、可靠性要求较高；由于需要接入内网，因此只能采用无线专网传输。

10）基建现场视频监控

施工现场视频监控系统为临时性部署业务，每路标清监控视频对带宽要求为2Mbps左右，对实时性、可靠性要求较低；具备条件的区域，应采用光纤或无线专网直接接入内网，无专网的区域，可以采用无线公网方式经过安全平台接入内网。

5.2 终端通信接入网业务对接入技术的需求分析

5.2.1 各种接入技术分析

终端通信接入网各种接入技术需求特征对比分析如表5-1所示。

表5-1 不同接入技术比较

技术名称	优　　点	缺　　点	适合应用场景	适合组网位置	适合承载业务
EPON技术	（1）带宽高、系统容量大、覆盖范围大、扩展性好； （2）可靠性高、实时性高、安全性高	建设成本较高	（1）适合新建/改造配电线路或线路通道具有铺设光缆条件； （2）具有较高业务通信需求	10kV通信接入网 0.4kV通信接入网	配电自动化、用电信息采集、电动汽车充电、分布式电源
工业以太网技术	（1）带宽高、系统容量大、覆盖范围大、扩展性好； （2）可靠性高、实时性高、安全性高	建设成本较高	（1）适合新建/改造配电线路或线路通道具有铺设光缆条件； （2）具有较高可靠性和实时性通信需求	10kV通信接入网	配电自动化，用电信息采集、电动汽车充电、分布式电源

续表

技术名称	优　　点	缺　　点	适合应用场景	适合组网位置	适合承载业务
230M专网技术	（1）230MHz为电力专用频点；（2）建设成本较低、施工简便	（1）带宽较低；（2）通信效果受地形影响大（小区地下室覆盖难度较大）	（1）适合覆盖广域范围提供窄带通信接入；（2）适合空间遮挡较少、终端节点较少的地区	10kV通信接入网0.4kV通信接入网	配电自动化（二遥）、用电信息采集
中压电力线载波技术	（1）建设成本低、施工简便；（2）专网运行、安全性高	（1）带宽低；（2）受到配电线路运行情况的影响，可靠性较低	（1）适合没有光缆且近期没有光缆改造计划的地区；（2）业务通信需求水平较低	10kV通信接入网	配电自动化（二遥）
低压电力线载波技术	（1）建设成本低、施工简便；（2）专网运行、安全性高	（1）带宽低；（2）传输距离较短；（3）受到配电线路运行情况的影响，可靠性较低	（1）适合低压接入；（2）适合不具备敷设光缆条件的原有配电网	0.4kV通信接入网	用电信息采集
公网无线技术	（1）建设成本低、施工简便；（2）应用范围广、可用性高	（1）运行费用高；（2）实时性和安全性较低	适合应用在多种专网通信技术均不易应用的地区	10kV通信接入网0.4kV通信接入网	配电自动化（二遥）、用电信息采集（作为远程通道）

5.2.2　终端通信接入网新技术

1. 北斗短报文通信技术

北斗卫星通信系统是全球首个在定位、授时之外具备报文通信功能的卫星导航系统，它的短报文通信功能是美国GPS和俄罗斯GLONASS都不具备的特殊功能。北斗卫星短报文通信具有用户机与用户机、用户机与地面控制中心间双向数字报文通信功能，一般的用户机可一次传输36个汉字，申请核准的可以达到120个汉字或240个代码。短报文通信功能不仅支持点对点双向通信，而且其提供的指挥端机可进行一点对多点的广播式传输，为各种平台应用提供了极大便利。北斗短报文通信功能提供了紧急通道，此通道无时间限制，可以按照设定的时间间隔不断发出求救信息。

目前我国的北斗卫星导航系统已经实现了包括我国领土全境在内的区域覆盖，其精准的时空服务能力已经优于GPS系统，同时比GPS系统具有更高的安全性，并具有可提供短报文数据通信（北斗RD功能）的差异化功能。

北斗短报文通信技术在终端通信接入网中应用前景广阔。北斗短报文技术可以在无信号覆盖的沙漠、偏远山区以及海洋等人烟稀少的地区实现电力设备的信息采集与状态监测等功能，而且还可以提供紧急通信服务；在地震等灾难发生时，可以及时报告终端设备的

状态信息，下达控制命令，有效提高紧急救援效率。

2. NB-IoT技术

当前终端通信接入网主要通过载波通信、光纤通信、无线宽带技术与租用无线公网等来运行。其中，载波通信与无线公网的安全性较低，光纤通信网的施工难度较高，难于灵活变通，无线宽带技术会受天气或路径反射干扰，在使用中也有一定的局限性。物联网可以合理解决配电网中的终端通信问题，仅需将配电网中的设备及其附件联通至互联网，便可以完成配网的通信工作，并且可以实现配网的遥信、遥测、遥控等自动化技术。物联网主要应用在电力系统通信中的应急通信、配网自动化、智能电网等方面。物联网为电网实现智能化提供了很好的技术保障。

NB-IoT技术由华为、高通和Neul联合提出，NB-LTE技术由爱立信、诺基亚等厂家提出。NB-IoT提出了全新的空口技术，相对来说在现有LTE网络上改动较大，但NB-IoT是提出的6大CleanSlate技术中，唯一一个满足在TSG GERAN #67会议中提出的5大目标（提升室内覆盖性能、支持大规模设备连接、减小设备复杂性、减小功耗和时延）的蜂窝物联网技术，特别是NB-IoT的通信模块成本低于GSM模块和NB-LTE模块。NB-IoT使用了授权频段，有三种部署方式：独立部署、保护带部署和带内部署。全球主流的频段是800MHz和900MHz。NB-IoT属于授权频段，如同2G/3G/4G一样，是专门规划的频段，频段干扰相对少。NB-IoT网络使用的标准具有电信级别，是可以提供更好信号服务质量、安全性和认证等的网络标准，与现有的蜂窝网络基站融合更有利于其快速大规模部署。运营商有成熟的电信网络产业生态链和经验，可以更好地运营NB-IoT网络。NB-IoT具有164dB的链路预算，GPRS的链路预算有144dB（TR 45.820），LTE是142.7dB（TR 36.888）。与GPRS和LTE相比，NB-IoT链路预算有20dB的提升，开阔环境信号覆盖范围可以增加7倍。20dB相当于信号穿透建筑外壁发生的损失，NB-IoT室内环境的信号覆盖相对要好。通常NB-IoT的通信距离是15km。NB-IoT具有连接更多、覆盖更广、功耗超低等优点，适用于智能抄表、智能停车、环境监测、智能物流、智慧城市等多种场景，已成为运营商蜂窝物联网的主流技术选择。

考虑到NB-IoT的特性，NB-IoT技术可以满足对低功耗/长待机、深覆盖、大容量有所要求的低速率业务；同时，由于对移动性支持较差，更适合静态业务场景或非连续移动、实时传输数据的业务场景，并且对时延低敏感，在终端通信接入网中，可以考虑的业务类型如下：

① 自主异常报告业务类型。如烟雾报警探测器、智能电表停电的通知等，上行数据极小数据量需求（十字节量级），周期多以年、月为单位。

② 自主周期报告业务类型。如智能公用事业（煤气/水/电）测量报告、智能环境等，上行较小数据量需求（百字节量级），周期以天、小时为单位。

③ 网络指令服务类型。如开启/关闭、设备触发发送上行报告、请求抄表，下行极小数据量需求（十字节量级），周期以天、小时为单位。

④ 软件更新业务类型。如软件不定期更新，上行下行较大数据量需求（千字节量级），周期多以天、小时为单位。

3. LPWAN

2016年全球使用64亿个物联网设备，每天将有550万个设备连网，而“万物互联”实现的基础之一在于数据的传输，不同的物联网业务对数据传输能力和实时性都有着不同要求。

根据传输速率的不同，可将物联网业务进行高、中、低速的区分：

① 高速率业务：主要使用3G、4G技术，例如车载物联网设备和监控摄像头，对应的业务特点要求实时的数据传输；

② 中等速率业务：主要使用GPRS技术，例如居民小区或超市的储物柜，使用频率高但并非实时使用，对网络传输速度的要求远不及高速率业务；

③ 低速率业务：业界将低速率业务市场归纳为LPWAN（Low Power Wide Area Network）市场，即低功耗广域网。

根据实际部署的调制方案LPWAN解决方案也存在很大的不同，比如超窄频带、窄频带和宽频带方案。超窄频带网络的发射端频带能够降低噪声，会给接收器端的敏感度、频带范围带来积极的影响，同时发射功率也更低一些。这些功能特性决定超窄频带系统所能实现的功能和应用场景，比如低数据速率、小型数据包、单向或者双向通信等。窄频带的网络则能够提供更好的适用性，对于频带范围和容量都具有广泛的适用性。另外，宽频带网络的频带在500kHz以上，最高能超过1MHz，因此它支持的数据速率也是最高的。

4. LoRa技术

LoRa是“Long Range”的缩写，由LoRa联盟维护管理，是一种基于物理层实现网络数据通信的技术，支持双向数据传输，符合一系列开源标准。它的网络实现具体解决方案称为LoRaWAN，是由Semtech公司（拥有核心芯片技术）开发的，由 IBM公司提供支持。LoRa技术采用chirp扩频调制技术，一个基站能够实现数百平方千米区域范围的网络覆盖。Semtech公司设计的SX1276低功耗长距离收发器可以应用于自动抄表、智能家居和楼宇自动化、无线预警和安全系统、工业监测和控制以及远程灌溉系统等。

这项技术能够实现多个通道不同数据速率的网络通信，主要与传输距离和所需求的消息持续时间有关。数据传输速率为300bps～50kbps，网络服务器和每个用户的物联网（IoT）设备终端的射频（RF）输出功率决定了数据传输速率。LoRa还提供了网络级、应用级和设备级的安全防护，适用于所有类型的双向通信物联网设备。

5. 毫米波无线技术

2.4G和5G频谱有越来越多的设备在使用，频谱资源越来越紧张，为了得到更高的

传输效率和频谱效率，需要新的无线技术。最近几年兴起了一种新的解决方案，能够解决现有频段面临的资源紧张问题，还能打破现有无线解决方案的各种限制。在毫米波（30～300GHz）频段中，60GHz频段因最具潜力脱颖而出。该频段在许多地区是免授权的，所以对于很多应用来说采用该频段是很方便的，相比目前已然十分拥挤的2.4GHz和5GHz频段能够提供海量的带宽。

在数据传输领域，60GHz技术可实现高达4.6Gbps的数据传输速率，比现有的802.11ac标准快5倍。办公楼宇与校园使用的无线回程应用依托60GHz数据传输，快速、便捷地构建楼宇和无线连接器之间的互连，实现了更加轻薄和稳定的设备。

60GHz频段频谱范围宽，能够提供千兆级的网络容量，并且该频段还具备多个关键的传播和衰减特性，全新的高性能无线解决方案可从中获益。包括美国FCC在内的监管机构已经为各行业划定了免授权频段。60GHz频段拥有超过7GHz的带宽，相较于5GHz频段，它能提供超过20倍的带宽资源。为了充分利用60GHz频段的优势，需要用到相控阵天线、定向度高的波束以及波束控制技术。

毫米波技术在未来的无线回程基础设施应用中也能够发挥重要作用，适用于下一代5G移动通信基础设施、固定接入回程扩展以及校园内的点对点链路等。60GHz通道的无线容量以及高度优化的射频链路可实现理想的“无线光纤”，用于替代现有的光纤回程应用。

目前市场上有多种方案在互相竞争，但大多数系统目前是基于IEEE 802.11ad标准实现的。除了之前提到的室内应用之外，对于现有802.11标准的修订涵盖了使用60GHz毫米波频段支持长距离链路（长达500m）应用。它使用为10米室内互连开发的同一波束控制技术，以支持接入点连接和室外回程链路等其他应用。

6. 异构网络

电力终端通信接入网终端数量不断增大，终端分布随机性增强，需要通信网络节点密集部署。在未来5G网络中，减小小区半径、增加低功率节点数量是电力终端通信接入网的核心技术之一。因此，异构网络成为未来电力终端通信接入网提高数据传输可靠性与实时性的关键技术。

未来无线网络将部署超过现有站点10倍以上的各种无线节点，在宏站覆盖区内，站点间距离将保持在10m以内，并且支持在每1km范围内为25000个用户提供服务。同时也可能出现活跃用户数和站点数的比例达1∶1的现象，即用户与服务节点一一对应。密集部署的网络拉近了终端与节点间的距离，使得网络的功率和频谱效率大幅度提高，同时也扩大了网络覆盖范围，扩展了系统容量，并且增强了业务在不同接入技术和各覆盖层次间的灵活性。虽然超密集异构网络架构在5G网中有很大的发展前景，但是节点间距离的减少，密集的网络部署将使得网络拓扑更加复杂，从而容易出现与现有移动通信系统不兼容的问题。在5G移动通信网络中，干扰是一个必须解决的问题。网络中的干扰主要有同频干扰、共享频谱资源干扰、不同覆盖层次间的干扰等。现有通信系统的干扰协调算法只能解

决单个干扰源问题，而在5G网络中，相邻节点的传输损耗一般差别不大，这将导致多个干扰源强度相近，进一步恶化网络性能，使得现有协调算法难以应对。此外，由于业务和用户对QoS需求的差异性很大，5G网络需要采用一系列措施来保障系统性能，主要有不同业务在网络中的实现、各种节点间的协调方案、网络的选择以及节能配置方法等。

7. 自组织网络

传统电力通信网络中，主要依靠人工方式完成网络部署及运维，既耗费大量人力资源又增加运行成本，而且网络优化也不理想。在未来电力5G终端通信接入网络中，将面临网络的部署、运营及维护的挑战，这主要是由于网络存在各种无线接入技术，且网络节点覆盖能力各不相同，它们之间的关系错综复杂。因此，自组织网络（self-organizing network，SON）的智能化将成为电力5G终端通信接入网必不可少的一项关键技术。

自组织网络技术解决的关键问题主要有以下2点：一是网络部署阶段的自规划和自配置；二是网络维护阶段的自优化和自愈合。自配置即新增网络节点的配置可实现即插即用，具有低成本、安装简易等优点。自优化的目的是减少业务工作量，达到提升网络质量及性能的效果，方法是通过UE和eNodeB测量，在本地eNodeB或网络管理方面进行参数自优化。自愈合指系统能自动检测问题、定位问题和排除故障，大大减少维护成本并避免对网络质量和用户体验的影响。自规划的目的是动态进行网络规划并执行，同时满足系统的容量扩展、业务监测或优化结果等方面的需求。目前，主要有集中式、分布式以及混合式3种自组织网络架构。其中，基于网管系统实现的集中式架构具有控制范围广、冲突小等优点，但也存在着运行速度慢、算法复杂度高等方面的不足；而分布式恰恰相反，主要通过SON分布在eNodeB上来实现，效率和响应速度高，网络扩展性较好，对系统依赖性小，缺点是协调困难；混合式结合了集中式和分布式两种架构的优点，缺点是设计复杂。SON 技术应用于移动通信网络时，其优势体现在网络效率和维护方面，同时减少了运营商的资本性支出和运营成本投入。由于现有的 SON 技术都是从各自网络的角度出发，自部署、自配置、自优化和自愈合等操作具有独立性和封闭性，在多网络之间缺乏协作，因此，研究支持异构网络协作的SON技术具有深远意义。

8. SDN/NFV

随着网络通信技术和计算机技术的发展，互联网+、三网融合、云计算服务等新兴产业对电力终端通信接入网在可扩展性、安全性、可控可管等方面提出了更高要求。SDN（software-defined networking，软件定义网络）/NFV（network function virtualization，网络功能虚拟化）作为一种新型的网络架构与构建技术，其倡导的控制与数据分离、软件化、虚拟化思想，为突破现有网络的困境带来了希望。在欧盟公布的5G愿景中，明确提出将利用 SDN/NFV作为基础技术支撑未来5G网络发展。SDN架构的核心特点是开放性、灵活性和可编程性。主要分3层：基础设施层位于网络最底层，包括大量基础网络设备，该层

根据控制层下发的规则处理和转发数据；中间层为控制层，该层主要负责对数据转发面的资源进行编排，控制网络拓扑、收集全局状态信息等；最上层为应用层，该层包括大量的应用服务，通过开放的北向API对网络资源进行调用。

未来电力终端通信接入网络中需要将控制与转发分离，进一步优化网络的管理，以SDN驱动整个网络系统。SDN将网络设备的控制平面从设备中分离出来，放到具有网络控制功能的控制器上进行集中控制。控制器掌握所有必需的信息，并通过开放的API被上层应用程序调用。这样可以消除大量手动配置的过程，简化管理员对全网的管理，提高业务部署的效率。SDN不会让网络变得更快，但会让整个基础设施简化，降低运营成本，提升效率。

5.2.3 终端通信接入网业务与接入技术匹配度分析

1）配电自动化业务

A+类区域以配电自动化三遥业务为主，优先采用光纤通信或无线专网。

A类区域包括三遥、二遥业务，应灵活选择光纤、无线或载波通信，三遥终端优先选择光纤通信和无线专网。

B类区域以二遥业务为主，C、D、E类区域采用二遥方式，考虑网络建设经济成本因素，宜采用无线公网承载为主、其他通信方式为辅的通信方式。

2）用电信息采集业务

用电信息采集业务中专变采集终端接入技术选择对通信网络的实时性、可靠性、安全性要求较高，因此考虑网络性能指标因素高于网络建设经济成本因素，但同时需兼顾技术成熟度和产业链指标。专变采集终端对实时性、可靠性要求较高，无线公网时延波动性大，服务质量难以保障，载波易受环境干扰，稳定性较差，宜优先采用光纤或无线专网方式进行承载。

集中器对时延要求较低，重点考虑经济建设成本，同时兼顾网络性能指标。对于集中抄表终端和分布式能源监控终端，对实时性、可靠性要求较低，考虑成本因素，宜优先选用无线公网，未来可能绘制用电动态曲线，信息量将显著增加，2G无线公网与载波速率将难以满足业务通信要求，宜优先采用4G无线公网；在已有光纤资源或无线专网覆盖的区域，可采用光纤或无线专网方式进行承载。

3）分布式电源

380/220V低压接入的分布式能源站点，业务信息主要为用电信息采集计量信息，业务终端数量多，离散分布，在终端通信接入网资源已覆盖区域，应充分利用已有资源实现覆盖；在终端通信接入网资源未覆盖区域，考虑经济成本，优先采用无线虚拟专网。

4）电动汽车充电站（桩）

充电桩是电动汽车服务网络的末端充电设施，数量多，位置分散，对安全性、实时性要求一般，应首先考虑网络建设成本。当充电桩所在区域具备终端通信接入网络资源时，

可采用自建终端通信接入网络资源实现接入；当充电桩所在区域不具备终端通信接入网络资源时，采用无线公网（无线虚拟专网）接入车联网平台。

集中充电站由大量充电桩组成，对带宽及可靠性要求较高，网络性能指标高于网络经济建设成本，优先采用EPON或工业以太网交换机；保证带宽资源情况下，可考虑自建TD-LTE 1800MHz无线专网实现覆盖。

5）移动巡检

移动巡检业务需要实现巡检终端与巡检中心之间的通信，传输的数据包括文字、图片、视频等多种形式，带宽要求为：语音业务8～64kbps，视频业务384kbps～2Mbps，数据业务64kbps～2Mbps，语音和视频类业务对时延和可靠性要求较高。在无线专网覆盖区域优先采用无线专网，其他区域可以采用无线公网。

6）配网抢修

配电抢修业务用于采集和传输配电故障现场的语音、图像、视频信息，传输速率需求约为4Mbps，时延要求为百毫秒级。在无线专网覆盖区域优先采用无线专网，其他区域适合使用4G无线公网。

7）配电设备/环境状态监测

配电设备/环境状态监测目前的试点对带宽要求较低，实时性要求不高，单个接入点的速率需求约为几千比特每秒，传输时延为秒级，各种通信方式都可以匹配。未来规模化部署时，配电监测点数量庞大，监测位置分布分散，建议在无线专网覆盖区域优先采用无线专网，其他区域采用无线公网。

8）电能质量监测

电能质量监测对带宽的要求高于1Mbps，在电力光纤/无线专网覆盖范围内优先使用光纤/无线专网，其他区域适合使用3G/4G无线公网。

9）机器人巡检

机器人巡检的数据类型包括图像、设备诊断等信息，要求数据传输速率大于2Mbps，对通信时延、可靠性要求较高。变电站内巡检一般选择WiFi技术组网。在无线专网覆盖区域，可选用无线专网进行承载，其次为4G无线公网。

不同业务场景推荐采用不同的接入技术，如表5-2所示。

表5-2 终端通信接入网业务与接入技术匹配度分析

业　　务	业 务 场 景	匹配接入技术
配电自动化	A+类区域	以三遥为主，优先采用光纤通信或无线专网
	A类区域	灵活选择光纤、无线或载波通信， 三遥终端优先选择光纤通信或无线专网
	B、C、D、E类区域	采用无线公网方式为主，其他通信方式为辅
用电信息采集	专变采集终端（含负控）	优先采用光纤专网，也可采用无线专网
	集中抄表终端	各种通信技术均能满足现阶段要求，未来公司可能绘制用电动态曲线，信息量将显著增加，宜采用光纤专网、无线专网、无线公网4G通信网络

续表

业　　务	业务场景	匹配接入技术
用电信息采集	分布式能源关口计量终端	各类通信技术均可，宜采用无线公网
	接入380/220V电压等级分布式电源监控终端	宜采用无线公网
电动汽车充电站（桩）	集中充电站	宜采用光纤专网就近接入电力通信传输网络；在电力光纤网络无法覆盖的区域，可以租用VPN（互联网）
	充电桩	宜采用已有通信资源就近接入；无电力自建通信资源时，采用无线公网
移动巡检	移动巡检终端与巡检中心之间通信	在无线专网覆盖区域优先采用无线专网，其他区域可以采用无线公网
配网抢修	配网抢修指挥车与配网抢修平台	在无线专网覆盖区域优先采用无线专网，其他区域适合使用4G无线公网
配电设备/环境状态监测	监测终端与监测主站	无线专网覆盖区域优先采用无线专网，其他区域采用无线公网
电能质量监测	监测终端与监测主站	优先使用光纤/无线专网，其他区域适合使用3G/4G无线公网
机器人巡检	机器人至控制中心	在无线专网覆盖区域，可选用无线专网进行承载，其次为4G无线公网

5.3　终端通信接入网业务对传输速率的需求分析

5.3.1　10kV通信接入网业务传输速率需求

10kV通信接入网主要承载配电自动化及配变监测、电能质量监测、配电监控运行、分布式电源控制、配电线路视频监控等业务，并作为0.4kV通信接入网承载业务的上联通道。其承载业务通信速率需求的典型值如表5-3所示。

表5-3　10kV通信接入网承载业务通信速率需求典型值

业务类型	终端类型	通信速率（kbps）
配电自动化	开关站	6～30
	环网柜	1.8～5
	箱式变压器	1.8～5
	柱上开关	0.9～2.5
	柱上变压器	0.9～2.5
电能质量监测	配电线路	2～4
配电监控运行	配网重要节点	1000～2000

续表

业务类型	终端类型	通信速率（kbps）
分布式电源控制	例：32个遥测、16个遥信、4个电度量计	0.592
配电线路视频监控	线路运行状态监测	1000
	线路视频监测	3000

5.3.2　0.4kV通信接入网业务传输速率需求

0.4kV通信接入网主要承载用电信息采集业务、售电抄表、客户服务、电力需求侧管理、负责监控、电能采集管理和充电桩通信等业务。其承载业务通信速率需求的典型值如表5-4所示。

表5-4　0.4kV通信接入网承载业务通信速率需求典型值

业务类型	终端类型	通信速率（kbps）
用电信息采集	单相居民/单相一般工商业用户	4～5
	三相一般工商业用户	6～27
	大型专变用户	12～30
	中小型专变用户	10～25
	充电站计量、分布式电源接入计量	12～30

5.4　终端通信接入网系统容量需求分析

5.4.1　终端通信接入网业务流量模型

业务流量模型是分析流量流向、容量等指标的有效手段，具有结构清晰、便于计算的特点，在常规的流量模型分析中需要对业务断面进行定义，采用分层方式进行断面流量计算。断面业务指的是两个通信实体节点间所有传输的业务总和，其中包括到两个节点终结的业务，也包括经过两个节点传输的业务。每个业务断面都有两个相关的通信实体节点，在各个业务断面中，包括各种类型的传输业务。

1）配电自动化业务流量模型

配电自动化业务的流量包含220kV/110kV/66kV/35kV各电压等级的10kV出线流量，流量模型中应考虑各电压等级的站点数量及每个电压等级下的线路数量，依据10kV站点的基本数据流量，业务流量模型如下：

$$B_{a31}=\sum_{\text{站点类型}}(\text{站点数量}\times\text{线路数量}\times 10\text{kV站点数据流量})$$

2）电能质量监测业务流量模型

电能质量监测需采集每条线路的三相电压、三相电流6个信息，每个数据2个字节，共计12个字节，计及数据采集周期、数据记录周期及数据上送时长，业务流量模型如下：

$$B_{a32} = n \times 12 \times Samp \times T_r / T_p$$

式中，n为10kV线路数量；$Samp$为采样频率；T_r为数据记录周期；T_p为数据上送时长。

3）配电监控运行业务流量模型

配电监控运行业务流量包括视频监控业务、语音业务、数据业务通道流量，并计及每条10kV线路设置的监控点数量，业务流量模型如下：

$$B_{a33} = \left(B_{视频监控业务} + B_{语音业务} + B_{数据业务}\right) \times N_{监控点数量}$$

4）分布式电源接入业务流量模型

分布式电源接入业务流量应依据每条10kV线路的接入点数及每个分布式电源接入采集的信息量计算业务流量，业务流量模型如下：

$$B_{a34} = \sum_{10\text{kV线路数量}} \sum_{接入点数量} B_{接入系统流量}$$

其中，$B_{接入系统流量}$应根据每个分布式电源系统采集的信息量计算。

5）其他业务

为营销业务系统预留300M带宽。

$$B_{a35} = 300$$

综合上述分析，计及并发系数、网络冗余系数及可靠性系数，变电站至区县汇聚点的断面流量模型如下：

$$B_{a2} = \sum_{变电站数量} \left(B_{a31} + B_{a32} + B_{a33} + B_{a34} + B_{a35}\right) \times 并发比例 \times 网络冗余系数 \times 可靠性系数$$

区县汇聚点至主站的断面流量模型如下：

$$B_{a1} = \sum_{区县汇聚点数量} B_{a2}$$

5.4.2 典型业务流量分析

配电自动化系统主要采集开关站、环网开关箱、箱式变电站、柱上开关、柱上变压器等设备信息。配电区域划分为A+、A、B、C、D、E六类，并给出A+、A、B类区域的业务终端典型规模，为通信业务分析提供依据。根据上述要求，A+、A、B类区域变电站配电自动化终端数量如表5-5～表5-7所示。

表5-5　A+类区域变电站配电自动化终端数量（按纯电缆计算）

站点类型		单线路站点数量（个）	线路数量		需求	传输方式
			110kV变电站	35kV变电站		
开关站		2	36	24	三遥	光纤为主
开关站		2	36	24	三遥	光纤为主
环网单元		2	36	24	三遥	光纤为主
箱式变电站	控制类	2	36	24	三遥	光纤为主
	非控制类	0	36	24	二遥	无线公网为主

表5-6　A类区域变电站配电自动化终端数量

站点类型		单线路站点数量（个）	线路数量		需求	传输方式
			110kV变电站	35kV变电站		
开关站		2	36	24	三遥	光纤为主
环网单元		2	36	24	三遥	光纤为主
箱式变电站	控制类	2	36	24	三遥	光纤为主
	非控制类	1	36	24	二遥	无线公网为主
柱上开关	联络开关	1	36	24	三遥	光纤为主
	分段开关	0	36	24	三遥	光纤为主
	分支开关	1	36	24	二遥	无线公网为主
	分界开关	0	36	24	二遥	无线公网为主

表5-7　B类区域变电站配电自动化终端数量

站点类型		单线路站点数量（个）	线路数量		需求	传输方式
			110kV变电站	35kV变电站		
开关站		1	36	24	三遥	光纤为主
环网单元		1	36	24	三遥	光纤为主
箱式变电站	控制类	0	36	24	三遥	光纤为主
	非控制类	2	36	24	二遥	无线公网为主
柱上开关	联络开关	1	36	24	三遥	光纤为主
	分段开关	1	36	24	二遥	无线公网为主
	分支开关	1	36	24	二遥	无线公网为主
	分界开关	0	36	24	二遥	无线公网为主

配电自动化典型终端站点的数据流量如表5-8所示。

表5-8　配电自动化典型终端站点的数据流量

站点类型	遥信量	遥信帧长度（B）	遥测量	遥测帧长度（B）	遥控量	遥控帧长度（B）	电度量	电度帧长度（B）	10kV站点数据流量
开关站	66	336	40	272	15	76	28	268	608
环网单元	23	164	16	152	9	76	4	100	316
箱式变电站	15	132	14	142	6	76	2	86	274
柱上开关	13	124	11	127	2	76	0	72	251
柱上变压器	4	88	13	137	0	0	3	93	225

5.4.3 典型业务流量计算

1. 配电自动化业务流量计算

根据业务通信模型和配电自动化典型终端站点的数据流量的数据，A+、A、B类配电区域配电自动化业务变电站断面流量，分别如表5-9～表5-11所示。

表5-9 A+类区域变电站配电自动化业务流量

站点类型	数据流量（kbps）		并发比例	网络冗余系数	可靠性系数	汇总流量（kbps）	
	110kV变电站	35kV变电站				110kV变电站	35kV变电站
开关站	350.208	233.472	100%	1.5	2	1050.624	700.416
环网单元	182.016	121.344	100%	1.5	2	546.048	364.032
箱式变电站（控制类）	157.824	105.216	100%	1.5	2	473.472	315.648
合　　计						2070.144	1380.096

表5-10 A类区域变电站配电自动化业务流量

站点类型	数据流量（kbps）		并发比例	网络冗余系数	可靠性系数	汇总流量（kbps）	
	110kV变电站	35kV变电站				110kV变电站	35kV变电站
开关站	350.208	233.472	100%	1.5	2	1050.624	700.416
环网单元	182.016	121.344	100%	1.5	2	546.048	364.032
箱式变电站（控制类）	157.824	105.216	100%	1.5	2	473.472	315.648
柱上开关（联络、分段）	0	0	100%	1.5	2	0	0
合　　计						2070.144	1380.096

表5-11 B类区域变电站配电自动化业务流量

站点类型	数据流量（kbps）		并发比例	网络冗余系数	可靠性系数	汇总流量（kbps）	
	110kV变电站	35kV变电站				110kV变电站	35kV变电站
开关站	175.104	116.736	100%	1.5	2	525.312	350.208
环网单元	91.008	60.672	100%	1.5	2	273.024	182.016
箱式变电站（控制类）	0	0	100%	1.5	2	0	0
柱上开关（联络、分段）	144.576	86.4	100%	1.5	2	433.728	259.2
合　　计						1232.064	791.424

在表格中，按照如下标准：

① 终端站点基本数据流量根据“单线路站点数量×线路数量×单站点数据流量/数据采集周期”确定，同时需要保证一定的冗余。

② 网络冗余系数为网络管理开销、信息加密开销、网络抖动预留冗余。

③ 可靠性系数为网络接纳转移负荷的能力。配电自动化业务光纤通信要求双路由备份，因此可靠性系数为2。

$$变电站断面流量=\sum_{站点类型}单线路站点数量\times线路数量\times10kV站点数据流量\times并发比例\times网络冗余系数\times可靠性系数$$

以A+类区域变电站配电自动化业务流量110kV变电站开关站数据流量为例，110kV变电站开关站数据流量=2（A+类区域单线路开关站站点数量）×36（线路数量）×608（10kV站点数据流量）=43776B/s =350.208kbps。则110kV变电站开关站汇总流量=110kV变电站开关站数据流量×100%（并发比例）×1.5（网络冗余系数）×2（可靠性系数）=1050.624kbps。同理，可以依次计算出A+类、A类、B类区域各站点类型的数据流量和汇总流量。

2. 其他业务流量计算

接入变电站的其他配电业务包含电能质量监测、配电运行监控、分布式电源接入，流量计算如下：

（1）电能质量监测

按每条线路1个监测点计算，每条线路采集信息量为三相电压、电流波形信息，采用连续监测方式进行监测，每次扰动数据在10s内上送到电能质量分析主站。每条出线按10kHz采样点数，记录2s的扰动数据，则每条线路上的业务净流量约为：

$$B_{电能质量监测}=（3\times2）_{三相电压电流}\times2B\times10kHz\times2s/10s=2.4\ kB/s=19.2kbps$$

（2）配电监控运行

按照每条10kV线路设置2个监控点计算，业务流量包括开闭所的视频监控业务、语音业务、数据业务通道。视频业务按4CIF格式计算，每个监控点2048kbps流量；语音业务每路按64kbps计算流量；数据业务包括就地操作票、工作票的接收和流转需求、门禁与温湿度等运行环境监控，按128kbps计算流量。

（3）分布式电源接入

按照每条10kV线路1个接入点计算，每个分布式电源点采集32点遥测，16点遥信，4点电度量计，计算方法与配电自动化业务相同。

110kV/35kV变电站承载的配电业务流量如表5-12所示。

表5-12　变电站其他配电业务流量

业务名称	终端流量（kbps）	数据流量（kbps）		并发比例	网络冗余系数	可靠性系数	汇总流量（kbps）	
		110kV变电站	35kV变电站				110kV变电站	35kV变电站
电能质量监测	19.2	36	28	100%	150%	1	1036.8	806.4
配电监控运行	2240	72	56	10%	150%	1	24192	18816
分布式电源接入	1.856	36	28	100%	150%	1	100.224	77.952
合计							25329.024	19700.352

（4）二遥终端无线公网承载流量

配电自动化业务中无线公网主要应用范围为：A、B、C类区域内的二遥配电终端通信传输；D类区域在具备三段式过流保护配合条件的主干线断路器且具有本地保护和重合闸功能的二遥配电终端通信传输。

采用无线公网通信的配电自动化业务不在变电站汇聚，经过无线公网通道直接接入配电自动化主站公网前置服务器，流量计算方法如表5-13所示。

表5-13　无线公网配电自动化业务流量

<table>
<tr><th>站点类型</th><th colspan="3">单条线路数据流量（kbps）</th><th>线路数量（条）</th><th>并发比例</th><th>网络冗余系数</th><th>可靠性系数</th><th>汇总流量（kbps）</th></tr>
<tr><td rowspan="2">A类变电站</td><td>箱式变电站（非控制类）</td><td>0.4384</td><td rowspan="2">0.84</td><td rowspan="2">N1</td><td rowspan="2">100%</td><td rowspan="2">1.5</td><td rowspan="2">1</td><td rowspan="2">0.97×N1</td></tr>
<tr><td>柱上开关（分支、分界）</td><td>0.4016</td></tr>
<tr><td rowspan="2">B类变电站</td><td>箱式变电站（非控制类）</td><td>0.8768</td><td rowspan="2">1.2784</td><td rowspan="2">N2</td><td rowspan="2">100%</td><td rowspan="2">1.5</td><td rowspan="2">1</td><td rowspan="2">1.91×N2</td></tr>
<tr><td>柱上开关（分支、分界）</td><td>0.4016</td></tr>
<tr><td>C/D类变电站</td><td>柱上开关</td><td>2.008</td><td>2.008</td><td>N3</td><td>100%</td><td>1.5</td><td>1</td><td>3.01×N3</td></tr>
<tr><td>合计</td><td colspan="8">0.97×N1+1.91×N2+3.01×N3</td></tr>
</table>

5.4.4　各类业务系统容量需求分析

变电站配用电数据流量既包含Ⅰ/Ⅱ区（生产控制大区）的配电自动化、电能质量监测、分布式电源接入等业务数据流量，也包括Ⅲ/Ⅳ区（管理信息大区）的用电信息采集、配电视频监控等业务数据流量。A+、A、B类配电区域变电站配用电数据流量汇总如表5-14～表5-16所示。

表5-14　A+类变电站配用电业务断面流量

<table>
<tr><th colspan="2" rowspan="2">业 务 类 型</th><th colspan="2">汇总流量（kbps）</th></tr>
<tr><th>110kV变电站</th><th>35kV变电站</th></tr>
<tr><td rowspan="4">生产控制大区业务</td><td>配电自动化系统</td><td>2070.14</td><td>1380.10</td></tr>
<tr><td>电能质量监测</td><td>1036.80</td><td>806.40</td></tr>
<tr><td>分布式电源接入</td><td>100.22</td><td>77.95</td></tr>
<tr><td>合计</td><td>3207.16</td><td>2264.45</td></tr>
<tr><td rowspan="4">管理信息大区业务</td><td>用电基本业务</td><td>6311.40</td><td>4181.30</td></tr>
<tr><td>用电扩展性业务</td><td>14730.30</td><td>9758.82</td></tr>
<tr><td>配电监控运行</td><td>24192.00</td><td>18816.00</td></tr>
<tr><td>合计</td><td>45233.70</td><td>32756.13</td></tr>
</table>

表5-15 A类变电站配用电业务断面流量

业务类型		汇总流量（kbps）	
		110kV变电站	35kV变电站
生产控制大区业务	配电自动化系统	2070.14	1380.10
	电能质量监测	1036.80	806.40
	分布式电源接入	100.22	77.95
	小计	3207.16	2264.45
管理信息大区业务	用电基本业务	6311.40	4181.30
	用电扩展性业务	14730.30	9758.82
	配电监控运行	24192.00	18816.00
	小计	45233.70	32756.13
合 计		48440.86	35020.58

表5-16 B类变电站配用电业务断面流量

业务类型		汇总流量（kbps）	
		110kV变电站	35kV变电站
生产控制大区业务	配电自动化系统	1232.06	791.42
	电能质量监测	1036.80	806.40
	分布式电源接入	100.22	77.95
	小计	2369.08	1675.77
管理信息大区业务	用电基本业务	6311.40	4181.30
	用电扩展性业务	14730.30	9758.82
	配电监控运行	24192.00	18816.00
	小计	45233.70	32756.12
合 计		47602.78	34431.89

为了统一计算标准，配电信息点假定如下：每个变电站32条配电出线，每条配电线路分别设置1个电能质量监控点、1个分布式电源监控点和2个视频监控点。每条配电线路按照柱上开关15台，开闭站2座，环网柜8座，箱式变电站30座，杆上变压器50台计算，共105个站点均需要实现配电自动化三遥业务，其中20个站点需要实现分布式馈线自动化高级业务。

按终端流量与变电站汇总流量2个层面来统计流量需求，终端流量指每个终端节点完成数据通信需要保证的流量，变电站汇总流量指每种业务所有终端节点汇总到变电站的数据流量。配电环节通信流量需求统计如表5-17所示。

表5-17　终端通信接入网配电环节通信流量需求

业务类型			终端流量（kbps）	终端数量（个）	并发比例	汇总流量（kbps）
配电自动化	三遥业务	开关站	15	2	100%	30
		环网柜	3	8	100%	24
		箱变	3	30	100%	90
		柱上变/柱上开关	1.5	65	100%	97.5
		合计		241.5		
	分布式馈线自动化		20	20	100%	400
电能质量监测（中压侧）			24	32	100%	768
分布式能源接入			2	32	100%	64
配变视频监控			8000	32	10%	25600
语音业务			64			64
合　计			基本业务流量1.47Mbps，含视频业务流量27.07Mbps			

分布式能源接入按IEC104通信规约每秒上传1次数据计算，根据每个接入终端点上送32点遥测，16点遥信，4点电度量计算信息量。

配变视频监控按覆盖到开关站计算，视频格式为1080p，单路需要4Mbps带宽，按10%的并发比例计算汇总流量。

为了统一计算标准，用电信息点假定如下：每变电站有100个台区，每台区有200个居民用户和6个工商用户，区域内有智能营业厅一座，电动汽车充电桩10个。通信流量需求按照远程通信信道和本地通信信道进行分析。配电环节通信流量需求统计如表5-18所示。

表5-18　终端通信接入网用电环节流量测算

业务	项　目		业务类别	字节数	台区数/终端数	并发比例	速　率
用电信息采集	上行	本地信道	居民单相电表	20	单台区单相终端200，三相终端6个，每整点抄收一次，窄带PLC 40min抄完	轮询，无并发	1.86kbps
			工商业用户三相电表	80			
		远程信道			单变电站100个台区，零点冻结数据15min内抄完	并发100%	497kbps
	下行	费控	远程	24	变电站100个台区，1h内下发	同时下发，速率267kbps；并发比例为10%，速率26.7kbps	
			本地	24	单台区206用户，假设1h下发完毕	轮询，无并发	1.37kbps
		遥信	远程				1.5kbps
		遥控	远程				1.5kbps

续表

业务	项　目	业务类别		字节数	台区数/终端数	并发比例	速　率
用电服务业务		智能营业厅					基本业务4.5Mbps，含视频业务12.9Mbps
		互动化用电			单台区100个用户实现互动化用电，每户速率最低256kbps，并发比例为10%，100个台区，并发比例为10%		25.6Mbps
		电动汽车充电	上行采集	80	充电桩10个，假设1min内抄完	100%	1.3kbps
			下行费控	24	充电桩10个，假设3min下发	100%	1.3kbps

5.5　终端通信接入网通信延时需求分析

5.5.1　不同业务类型通信延时要求

终端通信接入网中不同承载业务对接入网通信延时要求有较大的差异，根据终端通信接入网中不同承载业务对延时要求的不同，将各种承载业务按照延时分类如表5-19所示。

表5-19　终端通信接入网不同承载业务延时要求

位　置	业务名称	延时要求
配电业务	配网保护业务	＜40ms
	故障定位信息	
	SCADA遥信、遥测	＜500ms
	SCADA遥控、遥调	
	分布式能源站/储能站控制信息	
	分布式能源站/储能站状态监测	
	电能质量监测	
	遥视（视频监控）	＜2s
	电力设备运行状态监测信息	
用电业务	电动汽车充电桩	＞2s
	用电信息采集	
	负荷控制与管理	

5.5.2 终端通信接入网接入技术延时分析

终端通信接入网接入技术时延分析如下：

（1）EPON

当EPON系统仅承载以太网业务时，在业务流量不超过该系统吞吐量90%的情况下，其上行方向（ONU到OLT）的传输时延应小于1.5ms，下行方向（OLT到ONU）的传输时延应小于1ms（64～1518Byte）。

（2）工业以太网交换机

传输各种帧长数据时交换机固有时延应小于10μs；当采用环状网络时，以RSTP或MSTP恢复网络时每个交换机的最长时延不超过50ms。

（3）电力线载波

电力线载波采用主从轮询方式，实时性与网络节点数目有关，受信道质量、传输速率和传输协议限制；在使用窄带PLC时，物理层传输速率为10kbps的情况下，从载波机到主载波机的传输时延实测为1～2s，实时性较低。

（4）无线专网

无线专网时延与技术体制、网络负荷等因素有关。当负荷较大时，在不能划分专用通道的情况下，遥控业务需与其他业务分享信道资源时可能发生排队的情况，有可能无法满足实时性要求。目前可选技术（TD-LTE230、TD-LTE1800、McWill）的时延（无线终端至核心网）约为30～300ms。

（5）无线公网

传输时延与技术体制、公网负荷、终端分布、地域特点、气候环境等因素有关，需进行实际测试才能确定，传输延时一般约200ms。

上述通信技术的实时性比较如表5-20所示。

表5-20 终端通信接入网通信接入技术时延要求

通信技术	EPON	工业以太网	电力线载波	无线专网			无线公网（4G）
				TD-LTE 230	TD-LTE 1800	McWill	
业务延时	上行：1.5ms； 下行：1ms	10～100μs	0.4～2s	100～300ms	30～100ms	150～300ms	200ms
电力业务要求	1. 遥信/遥测上送主站的信息传送时间：光纤通信方式＜2s、载波通信方式＜3s、无线通信方式＜30s； 2. 遥控从确认执行到命令送出主站系统的间隔时间＜2s						

可以看出，EPON、工业以太网交换机采用光纤专线，实时性最高；中压载波由于信道可靠性以及受电力负荷影响较大，实时性较差；无线专网及无线公网选用的技术都较为成熟，无线专网实时性可以保障，无线公网服务质量与多种因素有关，实时性难以保障。

5.6　终端通信接入网业务安全稳定需求分析

5.6.1　安全防护需求

终端通信接入网络承载的业务主要有配电业务和用电业务，这些业务必须满足以下可靠传输及安全防护需求：

① 配电设备及部分用电通信设备大多运行在户外，需保障能在恶劣天气下正常工作，并能抵抗噪声、高电压、大电流、雷电等强电磁干扰，保持稳定运行。

② 高可靠性的信息传输通道，在电网线路故障或网络结构发生变化时不允许中断对配电设备的监测，即对配网系统的监测应不受线路故障和网络结构变化的影响。

③ 关键设备应进行冗余配置，单点故障不应引起系统功能丧失和数据丢失。

④ 防止通过串接方式、公共网络等对子站、终端进行攻击，造成用户供电中断。

⑤ 防止通过公共网络和配电终端入侵主站，造成更大范围的安全风险。

⑥ 保障重要数据的机密性、完整性。

⑦ 针对系统进行安全审计，指导信息安全的运维与管理工作。

5.6.2　业务安全分区

根据电力监控系统安全防护规定，发电企业、电网企业、供电企业内部基于计算机和网络技术的业务系统，原则上划分为生产控制大区和管理信息大区。生产控制大区可以分为控制区（安全区Ⅰ）和非控制区（安全区Ⅱ）；管理信息大区内部在不影响生产控制大区安全的前提下，可以根据各企业不同安全要求来划分安全区。生产控制大区内部的安全区之间应当采用具有访问控制功能的设备、防火墙或者相当功能的设施，实现逻辑隔离。在生产控制大区与广域网的纵向交接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关及相应设施。安全区边界应当采取必要的安全防护措施，禁止任何穿越生产控制大区和管理信息大区之间边界的通用网络服务。生产控制大区中的业务系统应当具有高安全性和高可靠性，禁止采用安全风险高的通用网络服务功能。依照电力调度管理体制建立基于公钥技术的分布式电力调度数字证书系统，生产控制大区中的重要业务系统应当采用认证加密机制。

因此，对于终端通信接入网中不同的业务安全性能指标的要求，可根据业务所处安全分区划分为生产控制大区和管理信息大区，如表5-21所示。

表5-21 终端通信接入网业务安全分区

业务属性	安全区域	业务名称
生产业务	Ⅰ区	调度自动化
	Ⅱ区	电能计量遥测系统、故障录波及双端测距、通信管理信息系统（统一监控、资源管理）
管理业务	Ⅲ区	变电站视频监视系统、光缆自动监测系统、通信机房监视系统、电能质量监测系统、通信管理信息系统（电子运维）、一次设备在线监测系统
	Ⅳ区	

5.7 终端通信接入网业务控制技术

5.7.1 基于业务等级的接入控制技术

无线接入控制是LTE系统中无线资源管理的一个重要内容。但无线接入控制只在新业务发起建立请求时或者当网络资源紧张时才发挥作用，分别决定接受哪个业务流的建立请求并允许其他接入或者终端哪个已有的业务流。接入控制一方面需要防止网络拥塞的出现，另一方面也需要在一定程度上保证已在系统中运行的QoS要求，并兼顾所有请求业务QoS意义下的公平。

无线接入控制对保证在某个小区内运行中的业务流的QoS起着重要作用，其采用的策略所遵循的一个重要原则是，仅当新业务流和已运行业务流的QoS要求都能得到满足时才允许新业务的接入。在LTE系统中的一种重要的承载级QoS参数为ARP，ARP可以根据资源使用情况决定是否接受承载的新建或者更改请求。因此，在LTE系统的无线接入控制中，ARP起着重要的作用。ARP用于指示分配和保留资源时的优先级，主要用于当资源有限的情况下决定哪个承载建立/修改请求可被接受或拒绝，以及哪个承载资源被释放。它包含三个必选子参数：

Priority Level：定义资源优先级，取值为1～15，等级1最高，等级1～8一般分配给运营商较高等级的业务，9～15用于漫游用户。

Pre-emption Capability：抢占其他已分配的较低优先级业务资源的能力，取值为yes或no。

Pre-emption Vulnerability：失去已分配的资源的能力，取值为yes或no。

由于ARP本身有15个取值，在核心网设置ARP优先级时，可以根据用户等级和所使用的业务综合设置Priority Level，PCRF可以根据策略要求对ARP进行修改。

表5-22显示了ARP参数与电力通信业务等级的映射。按照电力通信业务的优先级，将紧急业务、重点业务、标准业务、适度业务和ARP的各参数对应。其中，为了充分保证紧急业务和重点业务的传输，分别为它们分配了两个优先级，紧急业务的优先级为9、10，重点业务的为11、12。由于标准业务和适度业务对实时性的要求较低，因此它们分配到的优先级为13、14、15。对于优先级高（Priority Level值较小）的业务，eNodeB优先为其建立承载。在表5-22中，紧急业务和重点业务的Pre-emption Capability均为yes、Pre-emption Vulnerability的均为no，而标准业务和适度业务的则相反。这意味着资源不充裕时，紧急业务和重点业务具有抢占已分配给较低优先级业务的资源的能力，同时，低优先级的业务无法抢占已分配给这两类业务的资源。

表5-22 业务等级和ARP的映射

Priority Level	Pre-emption Capability	Pre-emption Vulnerability	电力通信业务
1～8			
9	yes	no	紧急业务
10			
11	yes	no	重点业务
12			
13	no	yes	标准业务 适度业务
14			
15			

图5-1表示了LTE无线接入控制的基本工作原理。

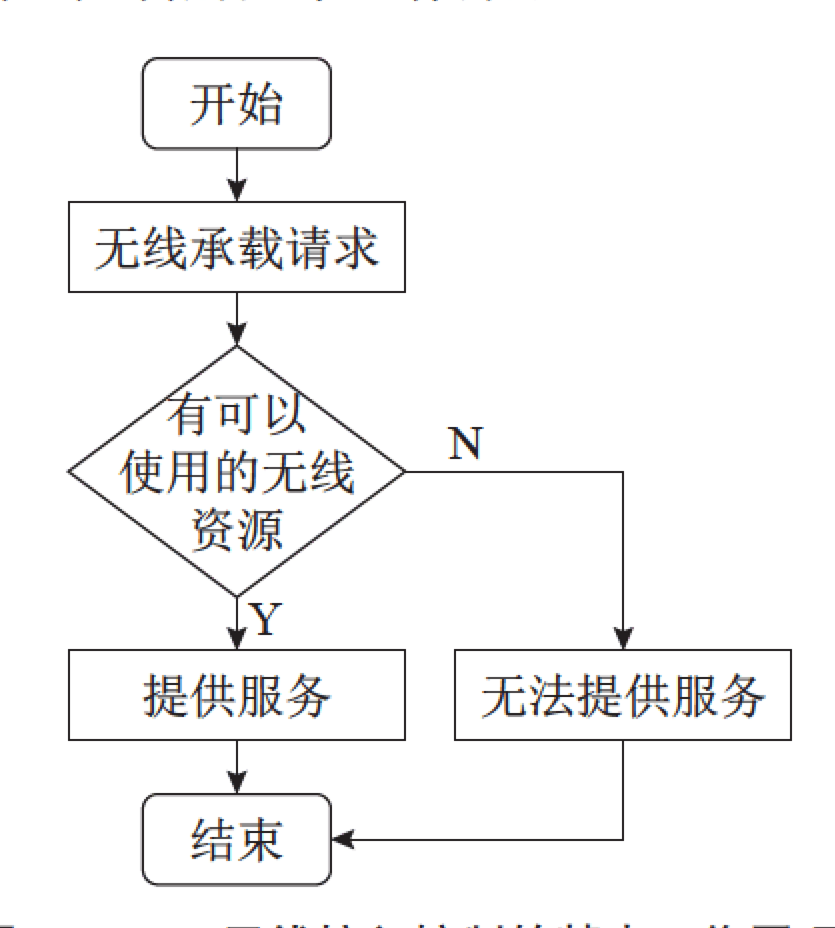


图5-1 LTE无线接入控制的基本工作原理图

LTE的无线接入控制在判断允许还是拒绝一个用户发起的无线承载的请求时，首先得判断用户业务的类型，着重考虑了用户业务的QoS需求后，优先级高的业务优先接入。然后对系统中的剩余可用资源进行估量，并与用户业务的需求进行比较，最终出现两种可能的结果：当系统目前可用资源小于用户业务的需求时，若发起请求的业务是高优先级的业务，如紧急业务和重点业务，系统可中断当前传输的低优先级的业务、适度业务和标准业

务，优先为高等级的业务建立承载；若发起请求的业务为低等级的业务，系统可拒绝业务的接入请求，一旦用户的业务被拒绝接入，则相应业务承载也就无法建立。当系统目前可用的资源多余的部分能够满足新用户业务的QoS需求，则新的用户业务请求被允许。之后，系统为这些新准入的用户业务流分配相关传输资源，进而建立相应的业务承载。

5.7.2 基于业务等级的分组调度技术

1. LTE的分组调度器

无线通信系统是资源受限的，如何利用有限的系统资源满足日益增长的用户需求，已经成为移动通信亟须解决的问题。如果没有有效的无线资源管理策略，再先进的传输技术，再宽的带宽也会因调度处理不合适而不能发挥其优势。分组调度就是针对不同分组的数据业务特性，对分组数据用户的业务进行管理和调度。分组调度要解决的基本问题是：当多个分组业务流等待接受服务时，必须确定合理的服务规则，安排业务流的服务顺序、服务时间以及传输分组使用的比特率，以满足各个业务流的QoS要求。

分组调度就是针对不同分组的数据业务特性，对分组数据用户的业务进行管理和调度。分组调度要解决的基本问题为：当多个分组业务流等待接受服务时，必须确定合理的服务规则，安排业务流的服务顺序、服务时间以及传输分组使用的比特率，以满足各个业务流的QoS需求。调度器是进行分组调度的功能实体。

一个好的调度算法要求在保护用户QoS要求的同时最大化系统容量，要兼顾系统的吞吐量与用户的QoS要求。

2. 基于队列等级的分组调度技术

LTE的调度器位于NodeB的第二层MAC层，作用是根据不同用户的QoS为其在共享信道上分享分配资源。物理层的主要作用是根据不同用户的信道质量选择调制编码方案、处理HARQ重传、传输块复用等。图5-2显示了LTE调度器的功能结构图。在调度过程中，UE和NodeB的交互过程为：NodeB向UE周期性发出下行链路参考信号，UE据此对信道质量进行测量并上报测量结果，NodeB在衡量QoS需求、队列长度以及UE上报的CQI（信道

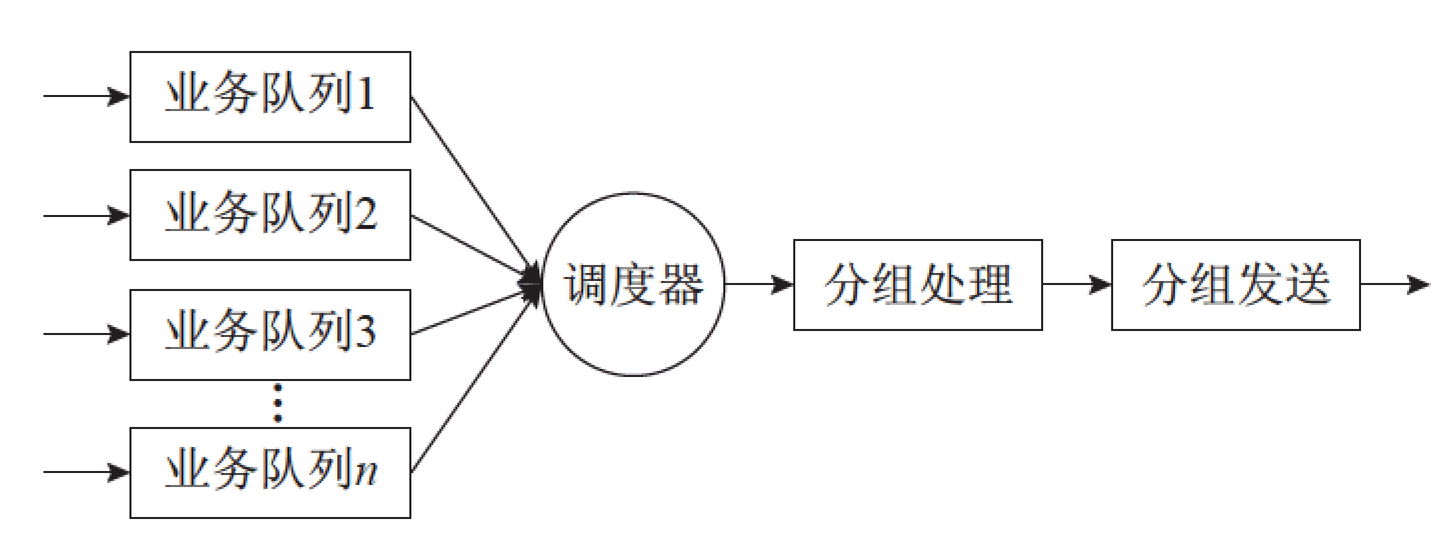


图5-2 LTE调度器功能结构

质量指示）等因素之后决定被调度的用户业务，并将调度结果和相关编码调制方案通过共享控制信道传输给调度的UE，接受调度的UE侧通过共享业务信道与NodeB进行数据交换。

LTE调度器应具有CQI报告控制、资源选择和分配、调度周期选择和优先级处理的能力。资源选择和分配指的是调度器决定为每个用户业务分配资源的数量、占用的有效时间以及资源所处的位置，并决定UE是采用集中式还是分布式的传输方案。对于资源调度周期选择功能，下行链路的资源调度周期应该为一个TTI（传输时间间隔）。另外，资源调度器应该能够根据缓存队列状态、CQI以及业务QoS要求等决定不同用户业务的调度优先级，即所述的优先级处理功能。

LTE调度器工作流程如图5-3所示，LTE系统中无线分组调度的主要流程概括如下。

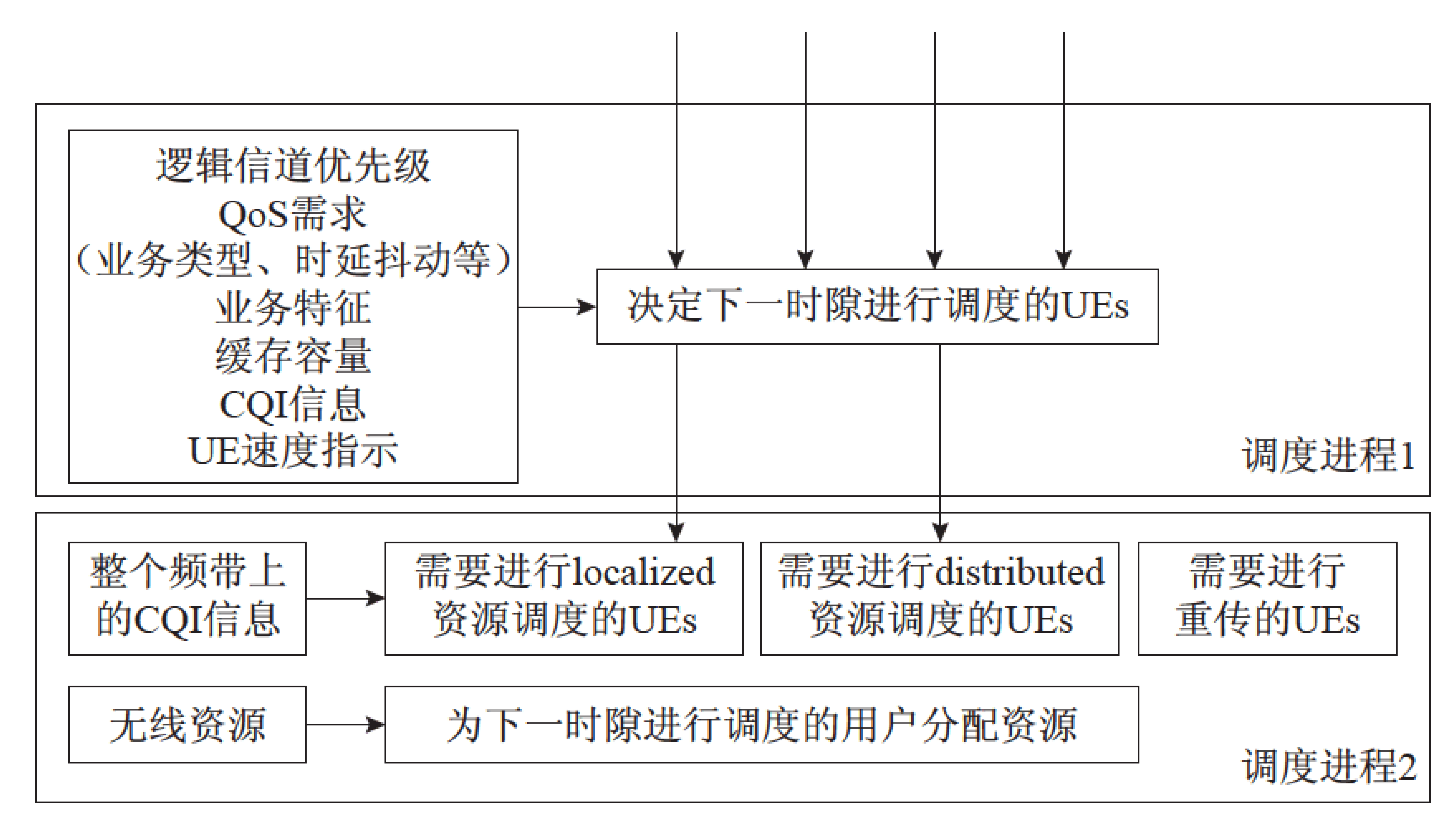


图5-3　LTE调度器工作流程

① 分别由物理层的信道状态检测模块、MAC层的缓存队列感知模块以及应用层的QoS需求模块获得当前信道的质量信息、缓存队列信息以及QoS需求信息。

② 在NodeB上的调度器根据搜集到的这些信息为每一个业务流计算优先级，得出下一个TTI的无线资源分配结果，并通过PDCCH信道告知每个UE。

③ UE根据被告知的资源分配结果在相应的时频资源块上进行数据传输。

5.7.3　基于业务等级的队列调度机制

1. 终端通信接入网业务优先级区分方法

终端通信接入网是电力骨干通信网的延伸，是实现电网智能化的关键所在，主要承载着配电自动化、配网调控一体化、用电信息采集等各项业务。随着智能电网建设的开展，为实现电力系统生产和管理信息的高度共享，在同一通信网络上传输各种保护、控制、管

理信息已成为智能电网发展的必然趋势。不同于当前多级多层次网络架构，构建一体传送的新型网架结构，势必将大大增加电力系统的信息传输量。如此，解决多种业务综合传输中的流量冲突问题，以保证各类业务的服务质量，特别要保证不同优先级下的业务服务质量将成为重中之重。

对于终端通信接入网而言，数据量的突发往往是由于紧急情况下高优先级业务的传输。这些突发的数据流将可能造成网络拥塞，使得转发节点成为整个网络的瓶颈，导致重要信息如故障告警信息、实时视频监控、配电自动化三遥数据等的时延增加。对于转发节点来说，时延过高又将会导致高优先级业务被丢弃。然而，高优先级业务往往意味着重要信息，这些业务如果被丢弃将可能影响到电网一次设备的动作，对电网造成很大的损失。

为了保障电网的安全稳定运行，必须保障高优先级业务的实时转发。在转发节点则主要考虑两个方面：一是对缓冲区长度进行划分，尽量减少分组被丢弃的可能性；二是优先转发这些重要业务，以缩小其转发时延。这就要求队列管理和队列调度策略相配合以达到保证服务质量的目的。然而，由于这类突发状态在终端接入通信网中比较少见，而且持续时间短，划分很大的缓冲区和带宽将造成严重的资源浪费。

为应对上述问题，决定通过变换不同队列的缓冲区长度来充分利用空闲缓冲区，减少突发数据流导致的分组丢弃，具有一定的抗突发能力。然而，当突发量较大时，由于突发流所属队列的分组到达速度大于其分组离开速率，导致队列发生拥塞，空闲缓冲区被迅速占满，一段时间后，在时间到达缓冲区更新点时，已经没有空闲缓冲区可供进行长度变换，导致上述队列管理算法失效，导致大量丢包。其次，上述队列管理算法虽然通过改变缓冲区长度减少了拥塞队列的丢包，但由于拥塞队列长度的不断增加，如果本队列的分组离开速率保持不变，则队列的分组时延会随着队列长度的增加而增加，不能满足高优先级队列相应的时延要求。为此，这里提出与上述队列管理算法相配合的动态权值队列调度算法（Dynamic Weight WFQ，DW-WFQ），通过限时队列缓冲区长度计算并改变队列权值，改变相应队列的分组离开速率，在拥塞时保证高优先级队列的时延需求。

此处以业务传输的紧迫程度为主，将其划分以下为三类：

F_1：紧急业务，如配网保护业务、故障定位信息。

F_2：重点业务，如三遥业务、调度电话、电力设备运行状态监测等。

F_3：适度业务，如用电信息采集、企业管理信息等。

2. BS-WFQ调度策略

BS-WFQ算法流程如下：

（1）计算队列发送速率

当新数据分组到达时，依照其所属队列当前的缓冲区长度，以公式更新权值ω_i：

$$\omega_i = \frac{L_i}{L_{i_0}} \omega_{i_0}, \quad i = 1,2,3 \tag{5-1}$$

其中，按照优先级由高到低，各队列的缓冲区长度分别记为$L1$、$L2$、$L3$，三者之和为缓冲区总长度$L0$，Li_0对应优先级队列Fi的缓冲区初始长度。各队列权值为$\omega_i (i=1,2,3)$，表示各队列在总发送速率中所占比例，$\sum_{i=1}^{3}\omega_i=1$，ω_{i_0}初始权值依照电力通信业务量比例分别为$\omega_{1_0}=0.1$，$\omega_{2_0}=0.2$，$\omega_{3_0}=0.7$。

式（5-1）表明，当限时缓冲区长度大于其初始长度时，表明此队列的分组到达速率较高，缓冲区较紧张，此时应增加队列的离开速率，以保证分组时延不受队列长度增加的影响，能够满足其时延需求；当缓冲区长度小于其初始长度时，说明此时队列进入速率较小，可以缩小此队列的权值。权值的动态变化能够按照当前队列状况更好地对调度顺序进行调整。

依照更新后的权值，计算此时队列分配的发送速率：

$$\lambda_i=\omega_i\lambda,\quad i=1,2,3 \tag{5-2}$$

（2）计算分组的截止时间

分组到达时间表示为T_{arrive}，分组所属队列的最大时延需求为$T_{\text{delay}i}$（$i=1,2,3$）。分组虚拟截止时间为$T_{\text{arrive}}+PL/\lambda_i$，其中$PL$表示分组长度，为简化问题，这里设数据分组长度相同，PL=1packet；分组所属队列满足时延需求的最大截止时间为$T_{\text{arrive}}+T_{\text{delay}i}$。

对于F_1与F_2，其分组最终截止时间为：

$$T_i=\min(T_{\text{arrive}}+PL/\lambda_i,T_{\text{arrive}}+T_{\text{delay}i}),\quad i=1,2 \tag{5-3}$$

这是为了保证有时延需求的分组的优先发送，避免发送过迟引起连锁反应，导致之后的分组不能及时发送导致时延过高。

对于F_3队列，由于没有时延需求，应当优先发送高优先级队列的分组，因此依照下式计算：

$$T_3=\max(T_{\text{arrive}}+PL/\lambda_3,T_{\text{arrive}}+T_{\text{delay3}}) \tag{5-4}$$

（3）判断并发送分组

各缓冲区中等待发送的分组均采用先进先出（FIFO）的方式进行发送。每次分组离开事件发生时，依次判断各非空队列中的首个分组，选择其中截止时间最小的分组进行发送。如果两个分组的截止时间相同，优先发送高优先级队列的分组。

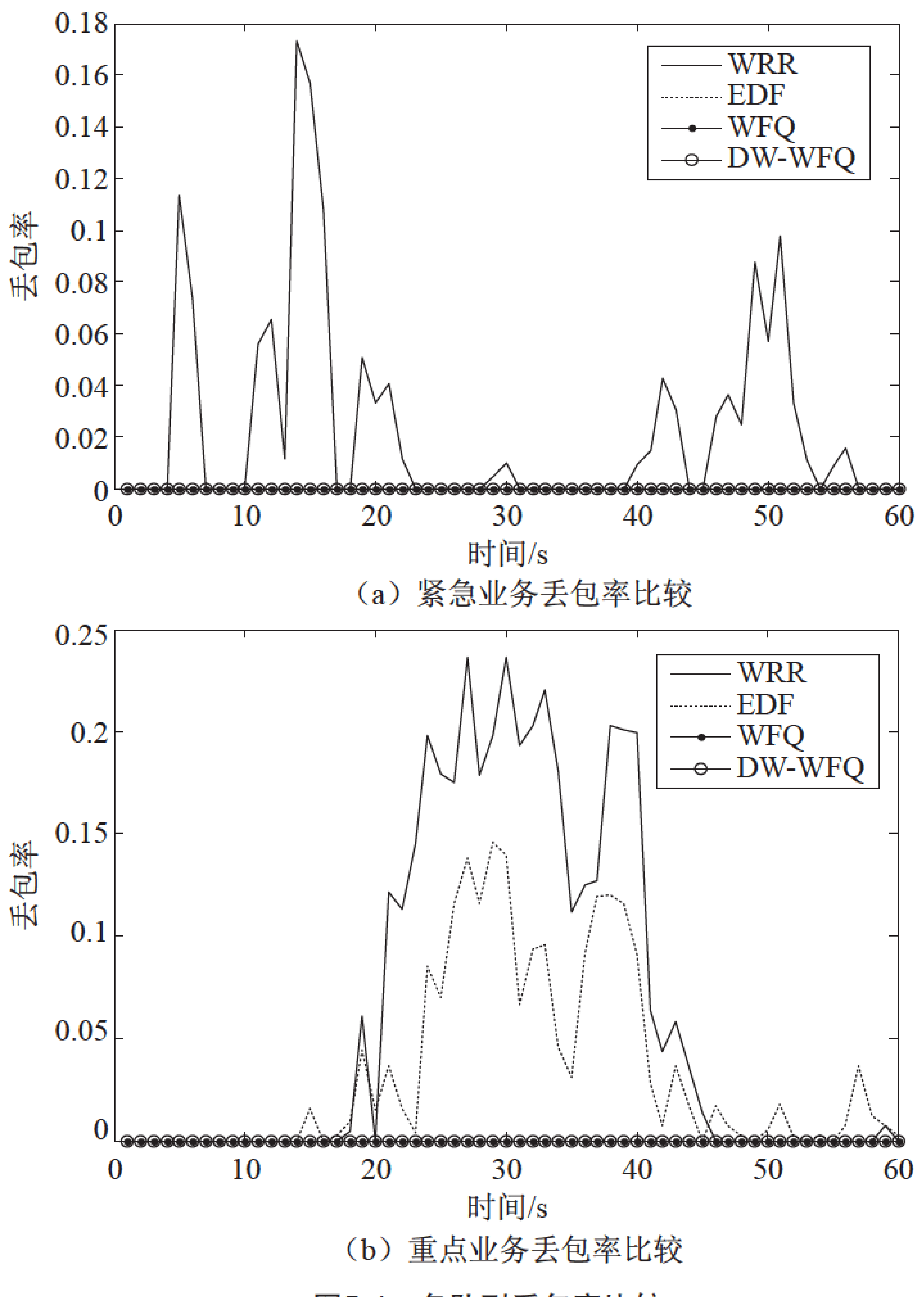
3. 仿真实验与结果分析

将三个等级业务的分组数量之比设为1∶2∶7。缓冲区总长度$L_0=500\text{packets}$，总缓冲区分为三份，初始值为$L_{1_0}=100\text{packets}$；$L_{2_0}=L_{3_0}=200\text{packets}$。各队列的最大时延需求分别设为10ms、100ms和1s。假设三个等级业务的分组到达速率服从参数为$\lambda_i (i=1,2,3)$的泊松分布，其中λ_1=200 packets/s，$\lambda_1:\lambda_2:\lambda_3=1:2:7$，仿真时间为60s，其中在0s、

20s、40s时紧急业务突发，突发量为100packets/s，持续时间均为20s。为保证无突发情况下路由器的进出平衡，总发送速率 $\lambda = 2000\text{packets} / \text{s}$。WRR算法的权值比为1∶2∶7。

1）丢包率

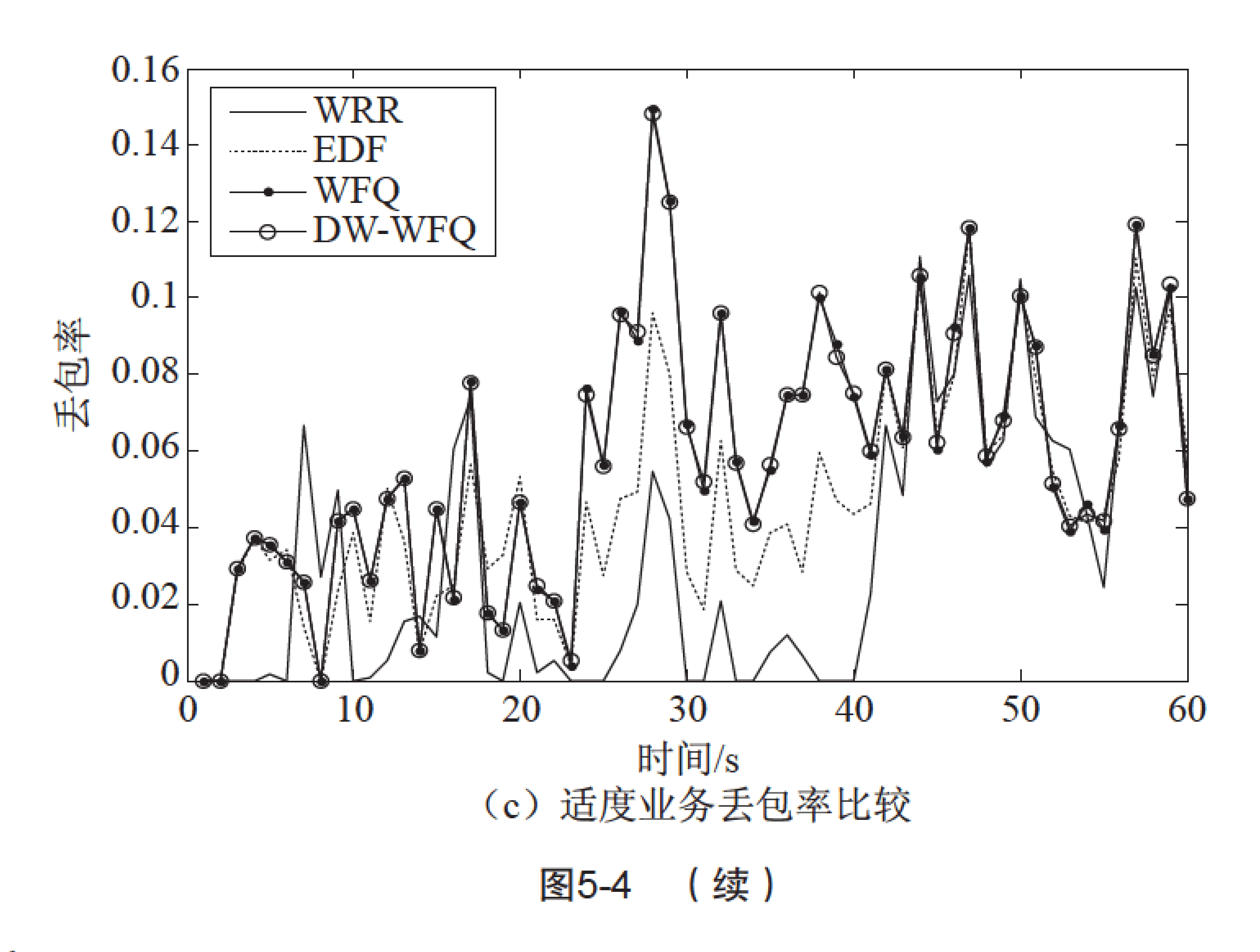
图5-4为四种调度算法的各队列丢包率比较曲线。由图（a）可以看出，除WRR算法外，EDF、WFQ与DW-WFQ算法均能维持EF队列的丢包率为0。由图（b）可以看出，对于重点业务，WFQ与DW-WFQ算法仍能维持丢包率为0；而EDF算法表现较差，主要丢包产生于20～40s内，数据量突发时，最高丢包率可达15%左右；WRR算法表现最差，尤其在20～40s时，WRR队列产生大量丢包，最高丢包率约为24%。由图（c）可以看出，WRR算法的适度业务丢包最少，EDF算法的高于WRR算法，WFQ与DW-WFQ算法的接近但更高，尤其在前40s，即EF与AF队列发生数据突变时，WFQ与DW-WFQ的丢包率明显高于WRR算法，这说明这两种算法牺牲了低优先级队列的服务质量，从而保证了高优先级队列的零丢包。



（a）紧急业务丢包率比较

（b）重点业务丢包率比较

图5-4　各队列丢包率比较



（c）适度业务丢包率比较

图5-4　（续）

2）时延

由图5-5可以看出，使用WRR算法进行调度时，EF队列的时延波动幅度很大，且最大时延接近1.5s，完全不能达到实时业务10ms的时延要求；而使用EDF算法前期时延满足要求，在约3000个分组之后，时延逐渐增加，直至约4000个分组后维持在70ms左右波动，最高接近90ms，虽然相比WRR算法有所进步，但距10ms的时延要求仍有相当的差距；使用WFQ算法和DW-WFQ算法后，EF队列的时延已远远低于10ms的时延要求，其中

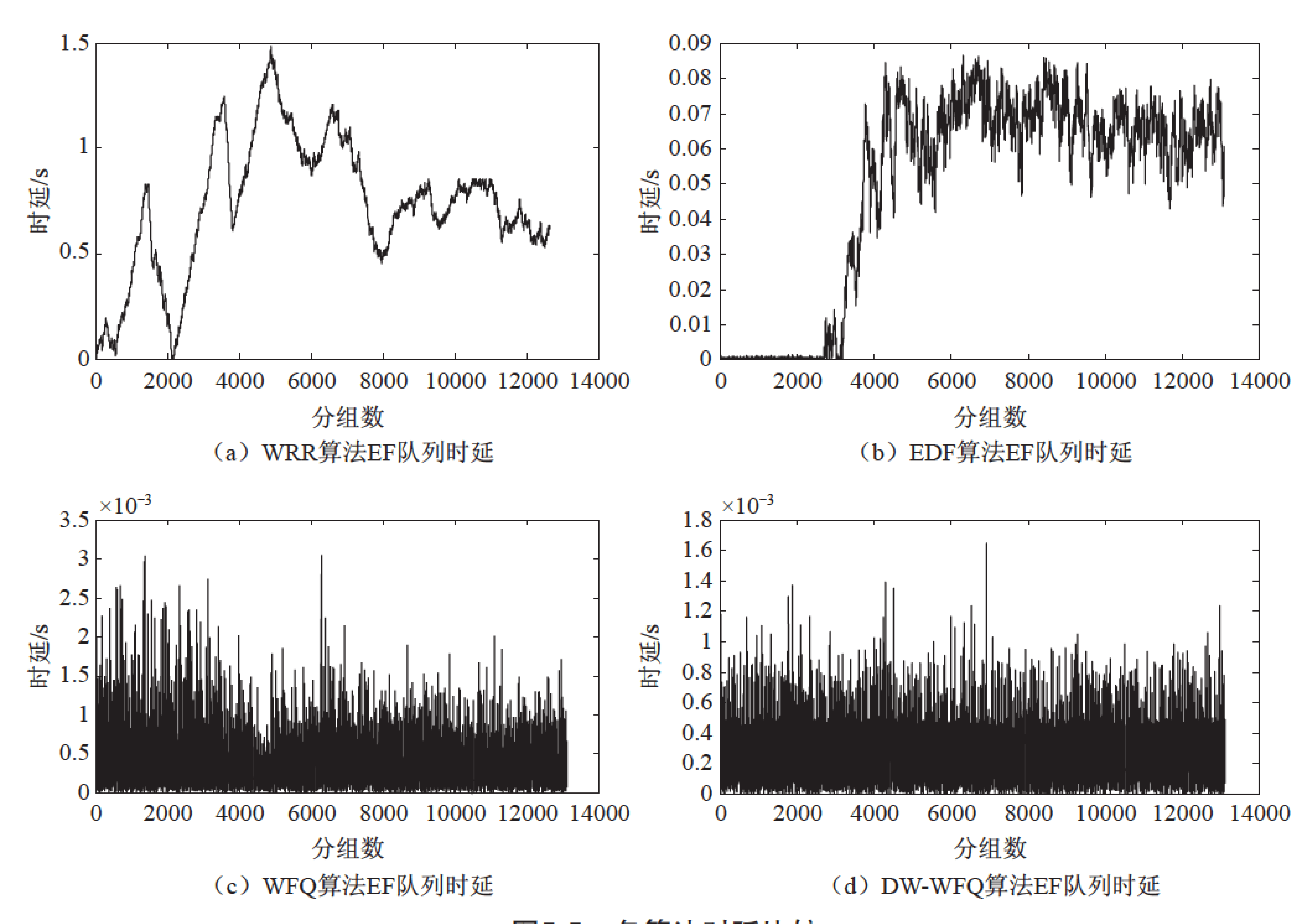


图5-5　各算法时延比较

WFQ算法的时延大部分在1.5ms以下，最高约3ms，且前期时延稍大于后期，这是由于前20s的分组到达速率较大，而队列权值未随之增加，因此队列的分组离开速率未变，从而导致时延稍有增加；而使用了DW-WFQ算法后，队列时延最高为1.6ms，基本位于0.8ms以下，并且在维持高优先级队列的低时延的同时兼顾了稳定性，表现更好。

3）缓冲利用率

图5-6为四种调度算法的缓冲区利用率比较曲线。由图中可以看出，使用WRR算法的缓冲区利用率波动较大，且在13s、20s和41s左右均达到90%以上，这说明此时队列缓冲区已接近全满，导致队列管理算法失效；EDF算法的缓冲区在经过一段时间后，利用率基本在80%～90%波动，说明缓冲区存在少量空闲可供队列管理算法进行调整，但调整力度非常有限；WFQ与DW_WFQ算法可维持缓冲区利用率在70%左右，说明有较多的空闲区域以预防突发数据流，但这是以增加低优先级队列的丢包率为代价实现的。

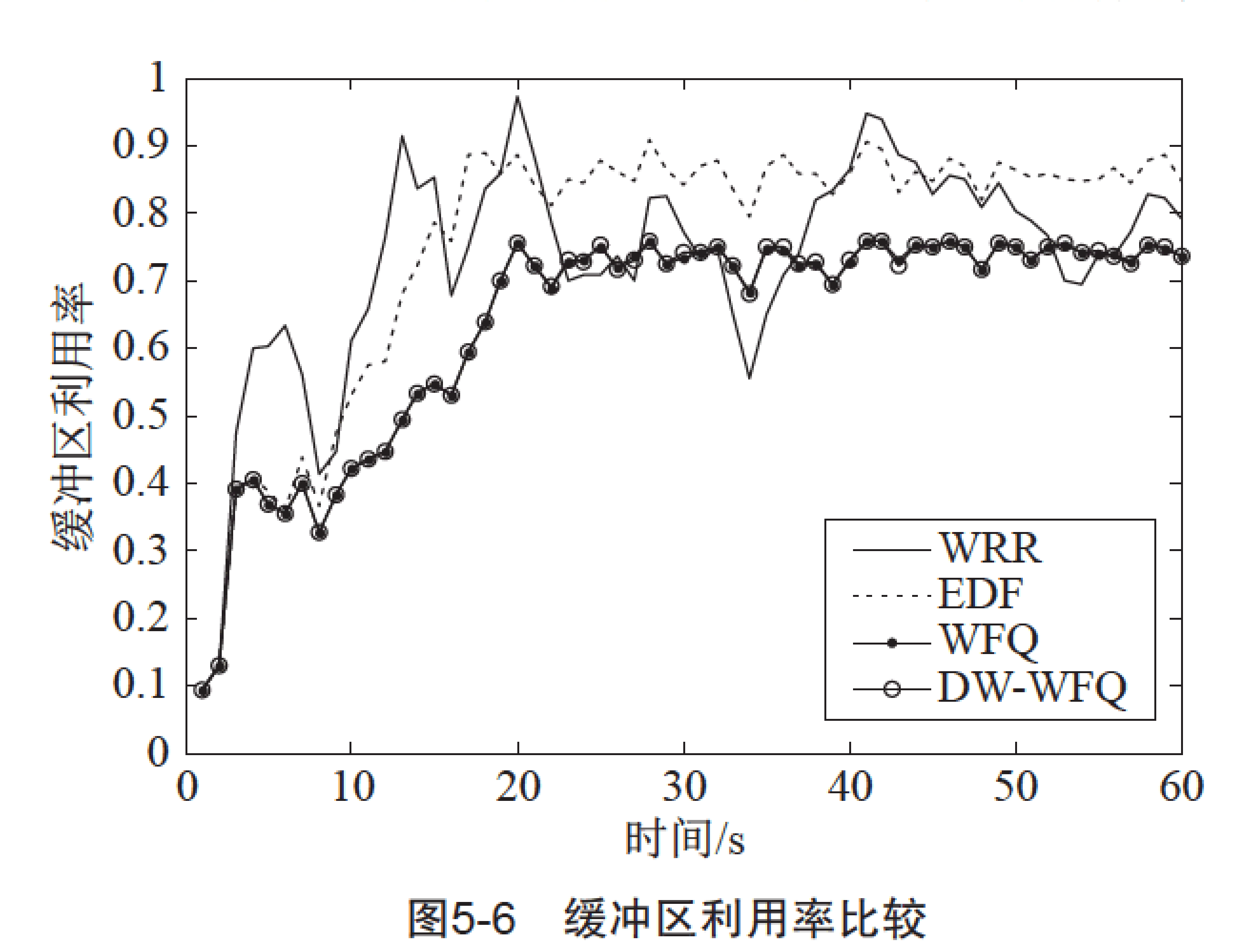


图5-6 缓冲区利用率比较

5.7.4 基于业务等级的队列管理机制

最早的拥塞控制机制出现在TCP协议中，由网络用户（通常为用户使用的传输协议，对于用户而言是透明的）根据丢包、超时等现象来判断网络是否出现拥塞，并采用慢速启动和拥塞避免算法来调整自己的数据发送速度，缓解传输网络的压力。随着显示拥塞通告（ECN）和主动队列管理（AQM）的思想的提出，拥塞控制不再只是网络用户的责任，在网络的传输节点中也引入了拥塞控制的机制。如何有效配合网络用户采用的协议，尽量避免拥塞的出现，如何区分出不遵守拥塞控制规范的网络用户，并限制其不止于影响其他用户和整个网络的有效运行等，都成为网络传输节点中的队列缓冲管理机制需要解决的关键问题。

通常情况下，为了提供有效的QoS支持，队列管理都放在输出端。缓冲管理机制位于队列的输入端，负责管理系统中缓冲资源的分配，根据系统策略和到达分组的信息来决定

是否允许其进入队列；而在队列的输出端，则有队列调度机制负责带宽分配和时延调整，两者互相配合完成完整的队列操作。而在队列操作机制之前，根据系统采取的策略和控制算法，可以辅助以分组分类、流量整形/调节等机制来配合队列管理机制的要求。

1. 基于业务等级的区分服务模型

目前的电力通信网络规模非常庞大，并且还在不断地延伸和拓展，因此其网络结构极其复杂。人们希望能在不改变现有网络结构的基础上，对网络进行所需的改造。因此，在区分服务（DiffServ）体系结构中，将整个网络划分成了多个DS域，每个DS域均处在同一个管理实体的控制管理之下，以此来实现相同的区分服务策略。DS域内的路由器分为外部路由器（External Router）和内部路由器（Interior Router）两种，所有复杂性工作都交给外部路由器进行处理，这样只需要在外部路由器增加区分服务功能即可，从而使内部路由器的工作更加简单，只需要对具有相同区分服务代码点（DSCP）值的数据流以相同策略进行转发即可。这样，内部路由器的转发机制得到了相当的简化，转发速率也因而得以提升。

数据流在进入外部路由器后，外部路由器对其进行分类、标记、计数测量等复杂性工作，然后将整理后的数据分组转发给内部路由器。内部路由器仅需依据分组的DSCP值进行转发，工作非常简单，从而使分组的时延、时延抖动、带宽和传送速率等QoS参数得以满足实际要求。因此，如果一个网络包含数个DS域，而每个DS域对于不同优先级业务均能满足其内部的QoS要求，则整体网络就能满足业务总体的QoS要求。

无论是外部路由器还是内部路由器，其工作内容都包括让分组进入队列，然后进行转发。当前，电力光通信网中数据流的数量持续增加，同时各种数据流的网络需求也不尽相同，而网络链路的带宽资源有限。因此，如何通过对数据流的管理和调度来合理优化对有限网络链路带宽的分配，一直是区分服务模型的研究重点。在优先保证高等级业务的时延、时延抖动和带宽等QoS参数的前提下，同时给予低等级业务一定程度的服务，这样通过合理分配各等级业务的转发，才能最大限度地优化网络的服务性能。

在区分服务模型中，对内部路由器在转发有优先级的业务数据流时相应的每跳行为（PHB）做出了规定。PHB可以使用队列管理与调度算法来实现，其种类与功能如下：

① EF PHB：加速转发PHB（Expedited Forwarding PHB）。EF PHB可以在DS域中实现低时延、低时延抖动和低丢包率以及确保带宽的端到端服务，适用于QoS需求高的实时性业务。

② AF PHB：确保转发PHB（Assured Forwarding PHB）。AF PHB可以保证一定的端到端服务质量要求。当网络发生拥塞时，在一定程度上保证数据分组得到最低限量的链路带宽。

③ BE PHB：尽力而为PHB（Best Effort PHB）。BE PHB只提供尽最大努力的服务，一般应用于没有硬性服务质量需求的一般数据流。BE PHB的优先级最低，但却是当今网络的主要服务模式。

2. 基于PLC-RED的端通信接入网主动队列管理算法

近年来，电力通信业务逐步迈向多样化、IP化、宽带化，人们对电力终端通信接入网的带宽容量、安全性及可靠性提出了更高的要求。目前IP业务已成为主流业务形态，AQM作为端到端拥塞控制的一种技术手段，一直是国内外学者的研究重点。但目前对AQM的算法仅从适应流与非适应流的角度来展开，依照数据流对路由器及链路的占用情况进行队列管理。对于电力系统通信业务来说，由于其业务复杂性日益增加，不同业务的服务要求也不尽相同。而生产运行类业务关乎整个电力系统的安全稳定，必须优先得到保证；企业管理类业务的服务要求则相对较低。因此，有必要将数据流依照服务质量要求划分为多个优先级进行差异处理。

针对终端通信接入网业务的自身特点，结合区分服务模型，提出一种改进的主动队列管理算法PLC-RED（Prediction and Length Change RED），通过预测并改变不同队列的缓冲区长度，在某一队列发生拥塞时，充分利用其他队列的空闲缓冲区，优先保证高优先级队列的服务质量，以达到降低整体丢包率、提高缓冲区利用率的目的。

1）算法描述

由于目前的电力通信网络模型可以分为集成服务（IntServ）模型和区分服务（DiffServ）模型，区分服务模型的特点是简单灵活、扩展性好，因此得到了较为广泛的应用。本项目采用区分服务模型，根据终端通信接入网业务不同的QoS要求，将数据流分为加速转发型（EF）、确保转发型（AF）与尽力服务型（BE）三种业务类型。其中EF型业务拥有最高的优先等级，在网络拥塞时也能够为用户提供高质量的服务保证；AF型业务等级低于EF型业务，当网络发生拥塞时能够提供一定量的服务质量保证；BE型业务则没有硬性的QoS要求，网络仅提供尽最大努力的服务，这也是当今网络所提供的主要服务模式。

首先将路由器缓冲区总长度记为L_0，依照EF、AF、BE型业务的长期平均业务情况，将总缓冲区划分为三部分，作为三种业务队列的初始缓冲区。EF、AF、BE型业务的缓冲区长度分别记为L_1、L_2、L_3。这里设L_0=500packets，L_1=100packets，L_2=L_3=200packets。每个队列均设置高低两个阈值$\max_i = \beta_i L_i$（$i = 1,2,3$）和$\min_i = \alpha_i L_i$（$i = 1,2,3$），α_i和β_i分别表示低阈系数和高阈系数，其中$0 \leqslant \alpha_i < \beta_i \leqslant 1$。

当新的数据分组到达路由器时，首先依据其区分服务码点（DSCP）值确定其分组类型及所属队列，如果所属队列已满则丢弃，如果还有空位则进入队列。

从0s计时开始，每经过时间t，标记一次时间，此标记点记为缓冲区更新点，这里设t=1s，而且每经$\frac{t}{n}$记录一次瞬时队长，记为q_i^k（$i = 1,2,3$；$k = 1,2,3,\cdots,n$），这里取$n = 10$。

每次到达缓冲区更新点时，进行缓冲区长度变换，流程如下：

（1）平均队列长度Avg_i计算

平均队列长度是指在一个周期内各取样时刻瞬时队列长度均值，其计算公式如下：

$$Avg_i = \frac{1}{n}\sum_{k=1}^{n} q_i^{k-n},\ i = 1,2,3 \tag{5-5}$$

（2）预测缓冲区长度 L_{Ei} 计算

预测缓冲区长度计算公式如下：

$$LU_i = Avg_i + \sum_{h=1}^{3} Numloss_i^{j-h+1}$$

$$L_{Ei} = LU_i / \gamma_i,\ i = 1,2,3 \tag{5-6}$$

其中 LU_i 表示第i个队列的预测队列长度，$Numloss_i^j$表示第i个队列在第j个标记周期内丢包数，$\gamma_i(\alpha_i < \gamma_i < \beta_i)$ 为预测系数，目的是给预测后的缓冲区留出一定余量，以应对预测误差。这里取 $\gamma_1 = 0.7$，$\gamma_2 = 0.8$，$\gamma_3 = 0.9$ 。同时，如果队列缓冲区过短，队列对新到达分组过于敏感，可能导致额外丢包，因此，各队列均设置有缓冲区长度下限 $l_i(i = 1,2,3)$，即经过长度变换后，其缓冲区长度不能低于其下限值。这里设 $l_1=l_2=l_3=60$packet。

（3）确定各队列缓冲区状况

比较L_{Ei}与队列高低阈值$\max_i$和$\min_i$的大小：若$L_{Ei}<\min_i$，表明队列处于闲置状态，需要缩短缓冲区长度；若$\min_i<L_{Ei}<\max_i$，表明队列无须变换缓冲区长度；若$L_{Ei}>\max_i$，表明队列处于紧张状态，需要增加缓冲区长度。

为了计算各队列缓冲区变化量各队列均设有缓冲区闲置长度 $Borrow_i$（i=1, 2, 3）和缓冲区紧张长度 $Loan_i$（i=1, 2, 3），其计算公式如下：

若队列缓冲区长度不足，则$Borrow_i=0$，$Loan_i=L_{Ei}-L_i$；若队列缓冲区长度过长：$Loan_i=0$，对于$Borrow_i$的计算则要比较此时的队列瞬时长度q_i，缓冲区长度下限l_i和预测缓冲长度L_{Ei}：当l_i最大时，$Borrow_i=L_i-l_i$；当L_{Ei}最大时，$Borrow_i=L_i-L_{Ei}$；当q_i最大时，$Borrow_i=L_i-q_i$；若队列缓冲区长度适中，则$Borrow_i=Loan_i=0$。

（4）各队列进行缓冲区长度变换

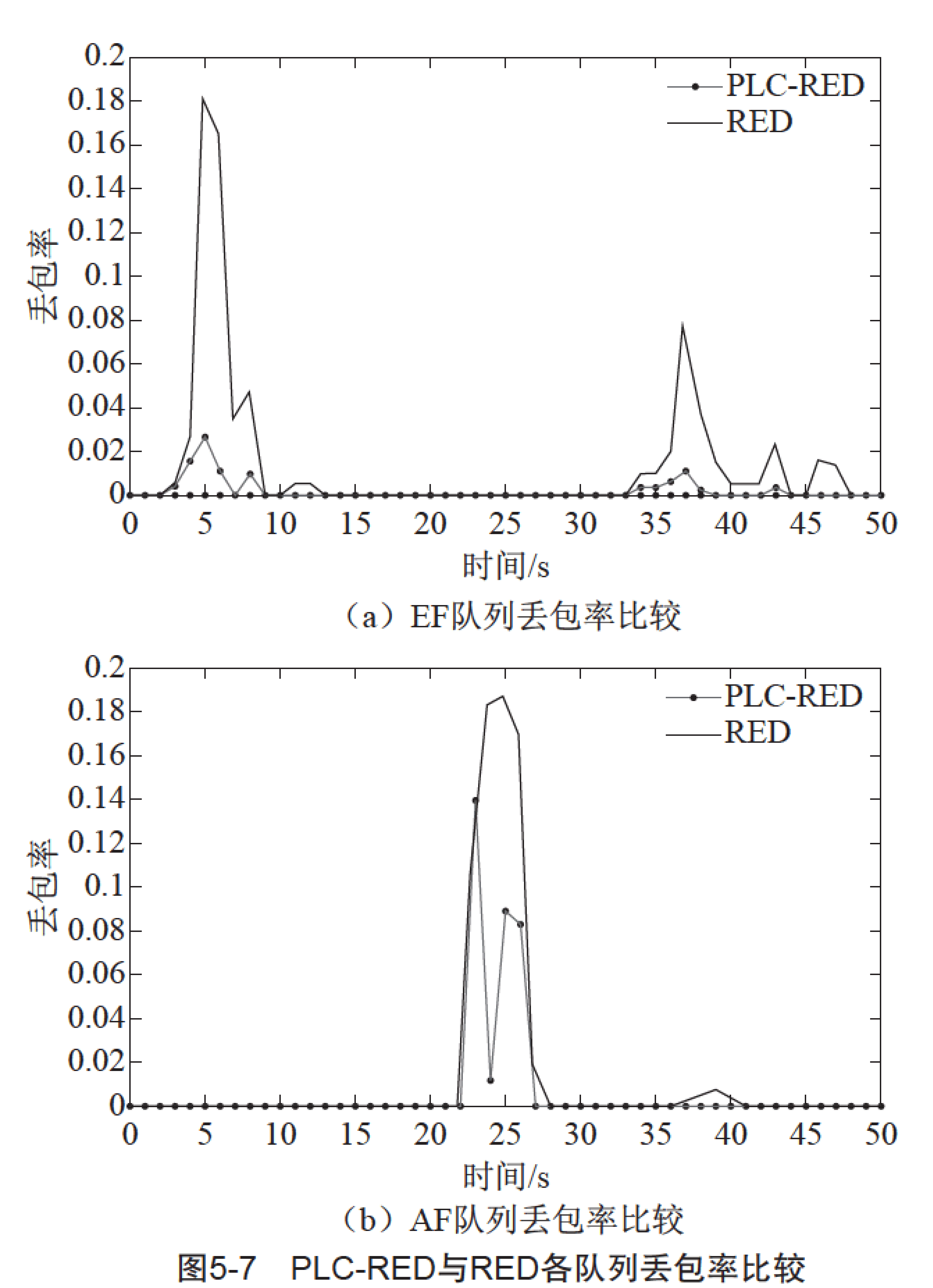
由EF队列开始，以优先级从高到低的顺序对三个队列依次进行判断：如果此队列处于紧张状态，即需要增加缓冲区长度，则以优先级从低到高寻找处于闲置状态的队列，增加紧张队列的缓冲区长度，同时闲置队列缩短相同长度，直至紧张队列能够满足其预测缓冲区长度或闲置缓冲区的闲置长度耗尽。如果本次变换过程中，三个队列均为闲置状态，则以优先级从高到低，对于现时长度小于初始长度的缓冲区，恢复其缓冲区直至初始长度或闲置缓冲区的闲置长度耗尽。

2）仿真结果与分析

在终端通信接入网中，通常高等级业务的业务量较少，相应的，低等级业务的业务量就多一些。因此，将三个等级业务的分组到达数量比设置为1∶2∶7。又，设三个等级

业务的分组到达速率服从参数为 $\lambda_i(i=1,2,3)$ 的泊松分布，且等级从高到低的参数之比也为1∶2∶7，仿真时间为50s，其中在0s、20s、40s时分别在EF、AF、BE队列发生数据突变，突发量分别为100packets/s，200packets/s，200packets/s，持续时间分别为5s，5s，10s。

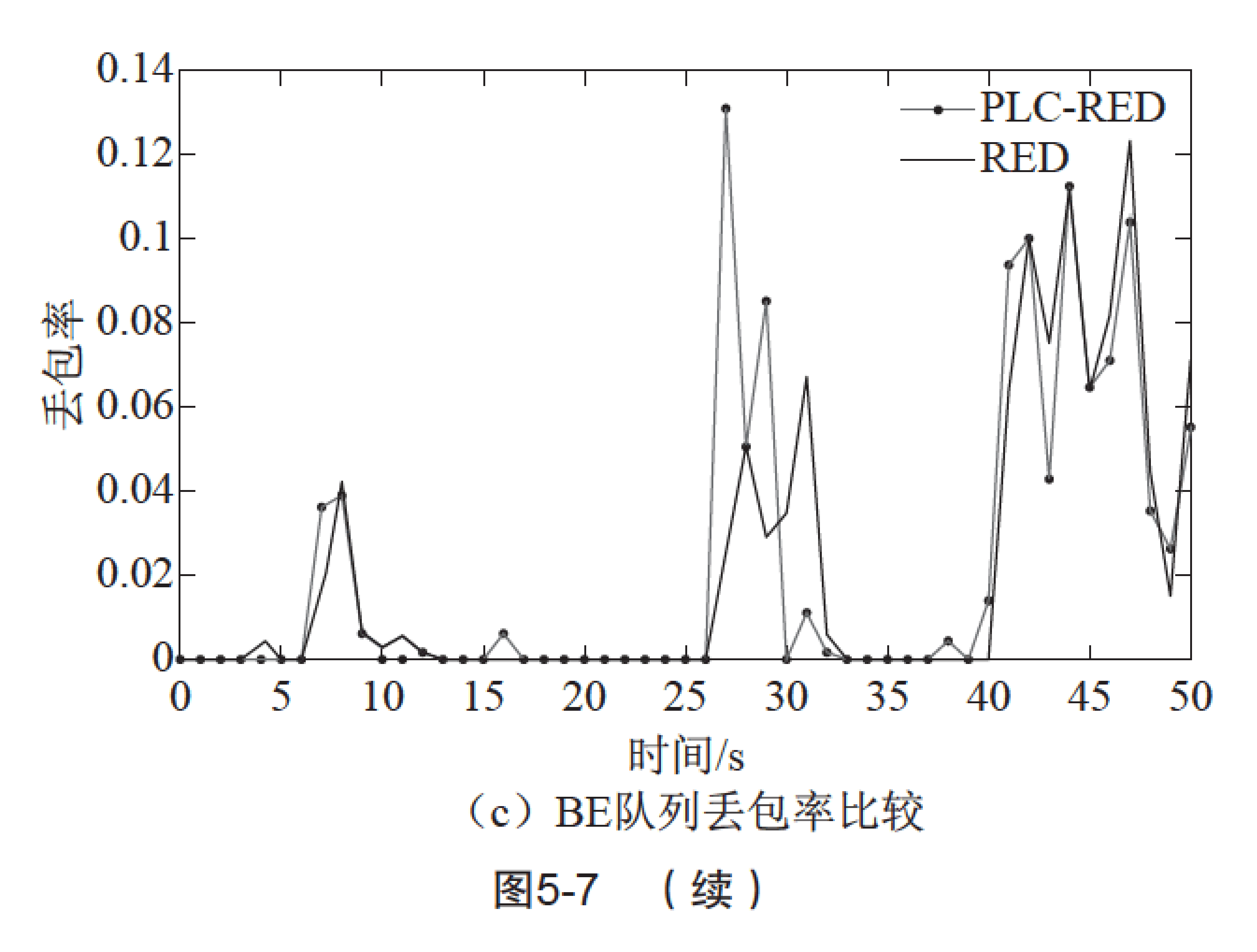
图5-7所示为改进后的PLC-RED算法与传统RED算法在各类型业务中运用时队列的丢包率比较。由图（a）可以清晰地看到，由于PLC-RED算法通过对缓冲区长度进行预测，在分组数量突变时，能够及时增加EF队列缓冲区长度，因此其EF队列丢包率远远小于传统RED算法。由图（b）也能够看出，由于同样的原因PLC-RED算法的AF队列丢包率要小于传统RED算法，但是相比于EF队列，丢包率却要高出很多，造成这样的结果一方面是由于突变量变大了，预测长度不足，另一方面是由于AF队列优先级要低于EF队列，增加缓冲区长度的优先级要低于EF队列。由图（c）可知，PLC-RED算法相比于传统RED算法，在BF队列中丢包率略高，甚至在26s处的丢包率远远高于传统RED算法，这是由于PLC-RED算法在本质上是以牺牲低优先级队列的缓冲区长度，来保证高优先级队列的容纳分组能力，因此在经长度变换后，BE缓冲区长度变短，使其平均队列长度容易达到队列高阈值，从而导致额外丢包。



（a）EF队列丢包率比较

（b）AF队列丢包率比较

图5-7 PLC-RED与RED各队列丢包率比较



（c）BE队列丢包率比较

图5-7　（续）

图5-8所示为两种算法整体丢包率的比较曲线，可以看出改进后的PLC-RED算法的整体丢包率明显比传统RED算法要低，说明PLC-RED算法不但能保证高优先级队列的服务质量，还能降低整体丢包率。

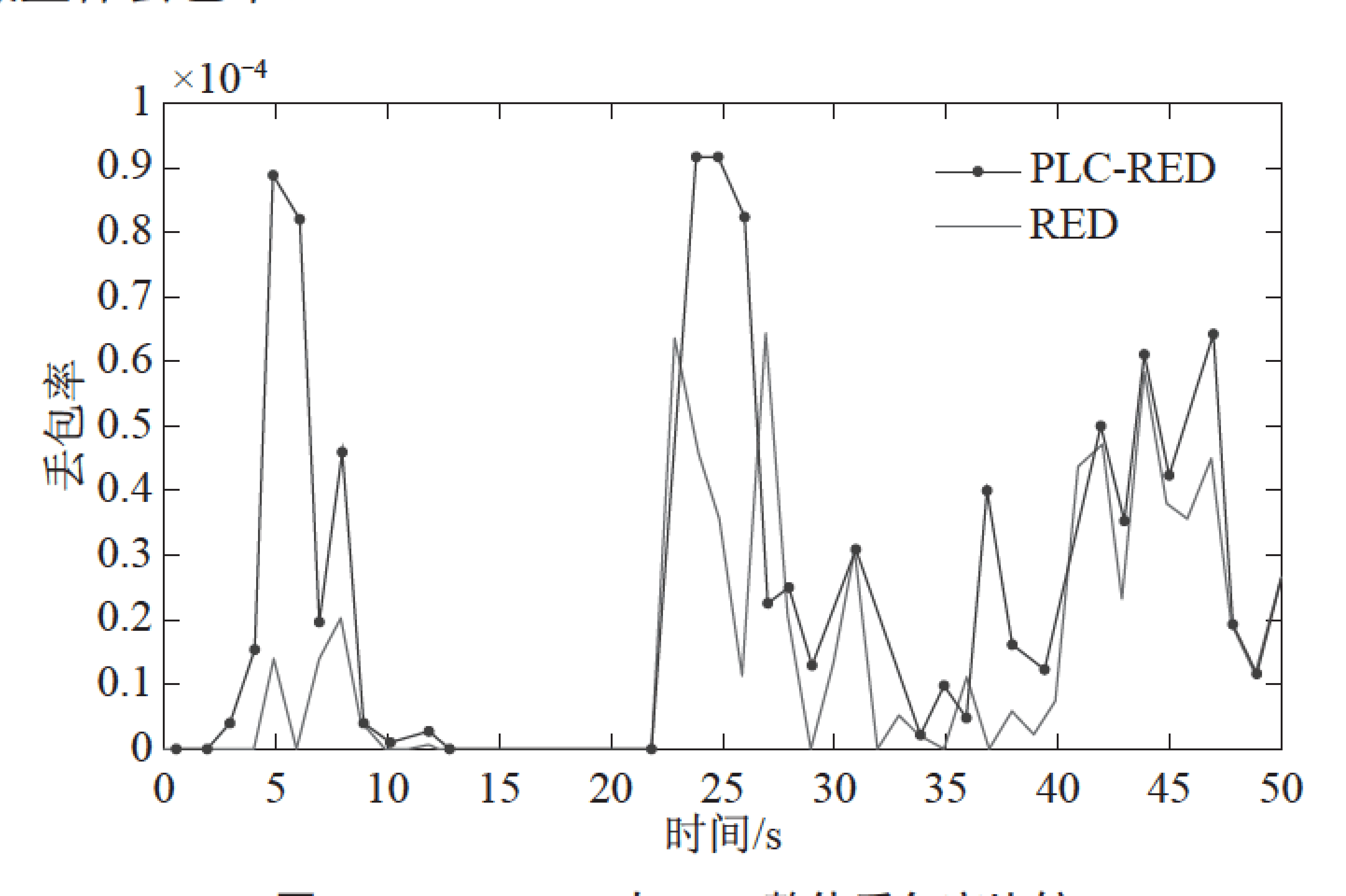


图5-8　PLC-RED与RED整体丢包率比较

图5-9所示是改进后的PLC-RED算法与传统RED算法的总缓冲区利用率曲线。从图中可以看出，在突变发生初期两者曲线基本重合，这是由于初始缓冲区长度在突变前期是够用的，不需要改变各队列的缓冲区长度，而随着突变的继续，PLC-RED算法的缓冲区利用率明显要高于RED算法，这是因为队列初始缓冲区不足时，RED算法只能通过丢包的方式去维持队列长度，而PLC-RED算法则能通过预测，并利用其他低优先级的队列空闲缓冲区，来提高总缓冲区利用率。

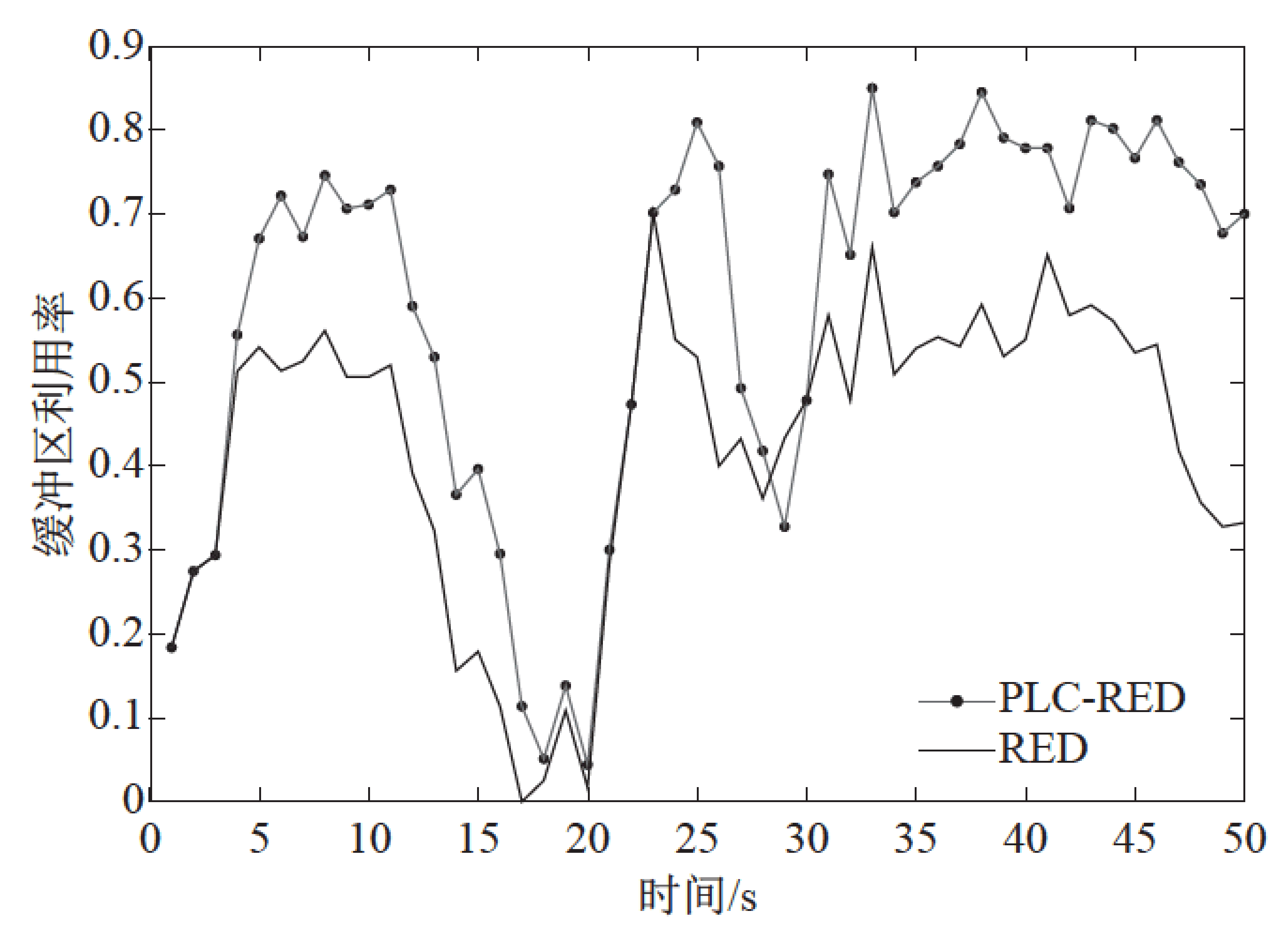


图5-9 PLC-RED与RED缓冲区利用率比较

由以上分析可知，PLC-RED算法对缓冲区长度进行预测并变换缓冲区长度，在高优先级队列发生数据拥塞时，通过牺牲低优先级队列的服务质量来换取高优先级队列的QoS要求，减少了高优先级队列丢包率和整体丢包率，并显著提高了这个路由器的缓冲区利用率。

5.8 终端通信接入网业务等级映射及QoS机制

5.8.1 EPON的业务等级映射及QoS机制

EOPN技术的QoS机制通过分配上下行通道的带宽实现，带宽的分配方案可分为静态带宽分配和动态带宽分配。

静态带宽分配对带宽采取固定配置的方式，系统按照各光网络单元（Optical Network Unit，ONU）预定的带宽进行初始配置，运行期间其值保持不变。其优点是实现简单，但存在带宽利用率低、带宽分配不公平、对突发业务适应能力差等问题。动态带宽分配对带宽采取实时调度方式，系统按照ONU实时上报的请求统筹安排，通过特定的算法动态地调整授权给ONU的带宽，保证各ONU上行数据帧互不冲突，从而充分利用系统资源，同时改善时延等性能。

基于动态带宽分配的优点，动态带宽分配（Dynamically Bandwidth Assignment，DBA）技术成为EPON的QoS关键技术。DBA是一种能在微秒或毫秒级的时间间隔内完成对上行带宽动态分配的机制，具有带宽效率高、公平性好、满足QoS要求的优点。其原

理为：光线路单元（Optical Line Terminal，OLT）的多点控制协议（Multipoint Control Protocol，MPCP）会下发轮询消息给ONU，ONU通过应答信息申请传送数据的所需带宽，OLT通过授权信息通知ONU在指定时间窗口发送数据，ONU通过授权信息通知ONU在指定时间窗口发送数据，ONU在指定的窗口打开激光器发送数据，发送完毕后关闭激光器。

EPON设备的带宽参数通过绑定DBA模板和线路模板来设置。DBA模板描述了EPON的流量参数，线路模板主要描述了逻辑链路标识符（Logical Link Identifier，LLID）和DBA模板的绑定关系。考虑到目前的上网业务下行速率的续期和重要性，OLT可以不设置ONU的带宽参数，以其他方式限制ONU的数据流的下行带宽。OLT的DBA模板分为5种模式，每一种模式都对应一种带宽分配方法。固定带宽是指任何情况下都被ONU占用的带宽。保证带宽是指ONU没有数据发送时，该部分带宽可被其他ONU使用，一旦ONU有数据发送，该部分带宽马上被占用。最大带宽是指ONU可以根据发送数据大小来分配的动态带宽。DBA模板的分类及说明如表5-23所示。

表5-23 DBA模板的分类

模 式	定 义	使 用 范 围
模式1	固定带宽	语音业务
模式2	保证带宽	视频业务
模式3	保证带宽+最大带宽	数据传送
模式4	最大带宽	上网业务
模式5	固定带宽+保证带宽+最大带宽	语音+数据传送+上网业务

1. IntServ和DiffServ体系架构

IntServ的基本思想是将所有业务的相关状态信息保存在端系统上，用资源预留的方式实现QoS保证。IntServ使用资源预留协议（RSVP）作为预留资源的信令协议，通过资源预留协议逐节点地建立或者拆除每个流的资源预留状态。在IntServ中，网络的管理力度是单个数据流，它定义了三种类型服务：确保服务（Guaranteed Services）、可控负载服务（Controlled-load Services）和尽力而为服务（Best-Effort），其中确保服务和可控负载服务对QoS有相应的要求，尽力而为服务没有任何QoS保证。IntServ能够提供端到端的QoS保证，但是由于IntServ的可扩展性太差，发送数据时要求发送端到接收端的所有路由器都支持RSVP，对路由器的实现要求太高，网络的管理变得复杂，资源利用率也会降低，因此IntServ服务模型只在数据流量较少的边缘网络中应用。

为了克服IntServ这一缺陷，IETF又提出了DiffServ模型。DiffServ通过在IP头设置DSCP（Differ Server Code Point）值将网络业务分为不同的行为聚类（Behavior Aggregate），对不同行为聚集类采取不同的逐跳转发模式（Per Hop Behavior，PHB）。在DiffServ中定义了两个有QoS保证的转发行为：保证转发AF PHB和快速转发EF PHB。

与IntServ模型相比，DiffServ具有实现简单、扩展性好的特点。但是DiffServ网络不能

给用户提供端到端的QoS保证，而且DiffServ中不能体现数据流之间的“微公平性”。目前，IntServ主要用于骨干网中。

1）IntServ和DiffServ结合的QoS机制

由于IntServ/RSVP和DiffServ各有长处和不足，且都不能完全满足IP网络的QoS需要，因此考虑将IntServ/RSVP和DiffServ两者结合，互相补充，进而实现端到端的QoS保证。

为解决RSVP在DiffServ域中的处理问题，IETF建议了两种互通方法来保证端到端的QoS，一种方法是将综合服务覆盖在DiffServ网上，RSVP信令完全透明地通过；另一种方法是简单的并行处理，即DiffServ域参与RSVP的协议处理。DiffServ网中的每个节点可能也是具有RSVP功能的，采取一些策略决定哪些包用RSVP，哪些包用DiffServ处理。相比而言，前一种方法实现简单，但却造成DiffServ域中的资源浪费，而且并没有完全实现端到端的QoS；后者相比于第一种方法要复杂一些，但是能够充分利用网络中的资源，能够提供端到端的QoS保证。

2）电力通信终端接入网的QoS机制

由以上分析可知，IntServ和DiffServ都难以满足IP网络的端到端的QoS需求，因此应将两者结合起来，在电力数据网中也是如此。电力通信业务能否准确及时地传输关系着电网能否正常运行。因此，电力通信业务对QoS有着很高的要求，而且电力通信业务种类多，单个通信终端传输的信息量少，但终端数据众多，总的传输数据量大。IntServ服务的最大优点是能够根据用户的实际需要，定制出完全符合用户需求的网络服务，具有相当的灵活性，适合网络规模较小、业务质量要求较高的边缘网络，适用于终端通信接入网，而它最大的缺点则是实现的复杂性，难以在核心网上大量使用，不适合用于核心网络。DiffServ服务恰恰相反，它最大的优点在于它在核心网上的可扩展性，其处理的对象是聚合流，有相同QoS要求的数据流聚合传输，降低了实现QoS保证的复杂性。为保证电力数据网端到端的QoS，可以把IntServ和DiffServ两种服务模式结合起来，在核心网中采用DiffServ模型，在接入网中采用IntServ模型，互相协同。两种服务模式结合时，需要考虑以下问题：

（1）业务映射机制

在IntServ区，业务被分为三类以区别QoS及为其提供的服务，而在DiffServ区使用DSCP来区分业务的QoS。DiffServ区要能够为标准的IntServ的QoS服务提供支持，必须实现两个区的业务映射。将IntServ的确保服务在DiffServ中映射为EF PHB；IntServ中的可控服务在DiffServ中转换为AF PHB，而对于IntServ中的尽力而为业务在DiffServ网络中不给予QoS保证，仅采取尽力而为转发。

（2）DiffServ/RSVP

DiffServ区确定一种机制对RSVP消息进行传递和处理，以保证能够为整个网络提供端到端的QoS。

下面以DiffServ核心网不支持RSVP协议的情况为例，来说明端到端QoS的具体实现过程：

① 发送端以信令方式发出PATH消息，与发送端相连的IntServ网络对PATH消息进行

处理。

② ER1用DS的方法将RSVP资源预留映射到响应的服务类别上，即与DSCP对应，并且将PATH消息发往DiffServ区域。

③ PATH消息在DiffServ核心网内透明地传输，然后在ER2上RSVP被重新启用。

④ 当PATH消息到达接收端主机时，它发送出RESV消息，以规范业务流所需要的资源。

⑤ 如果ER2认为与DiffServ区域相连的接口的资源不能满足所请求的资源，则ER2拒绝该请求，如果能满足要求的话，则将RESV消息透明地穿过DiffServ区域。

⑥ 在ER1处，RESV消息出发接入控制程序，它将从检查网络的可用资源以决定是否接受该业务流。如果ER1接受该请求的话，它将从RESV消息中获得数据包的DSCP值，开始向接收端发送标记了DSCP的数据包。

（3）资源管理

在DiffServ区的边界点执行适当的资源管理控制。DiffServ网络中的一部分，可以通过RSVP将DiffServ网络的可用资源的改变通知给DiffServ网络外部的IntServ节点。这样也可以根据DiffServ区外部的资源请求实现DiffServ网络内部资源的改变。

（4）接纳控制

DiffServ网络必须基于资源的可利用性，为客户（非区分服务区）网络提供接纳控制。DiffServ网络与IntServ/RSVP协同工作，可以实现基于策略的显示接纳控制。在DiffServ网络区采用RSVP接纳控制代理，可以在决定资源分配时，根据特定用户的业务需求，采取不同的资源预留策略，实现基于策略的接纳控制。

基于以上分析，可采用如图5-10所示的IntServ模型和DiffServ模型结合的QoS保证机制。在网络中央有一个DiffServ区，DiffServ区内部的一些路由器（BR1和BR2）支持RSVP，能够实现基于流的信令和接纳控制。DiffServ网络区内的路由器不仅支持RSVP信令，还能够对聚集传输流进行识别、分类和调度（聚集传输控制）。当一个新的数据流加入到行为聚集中时，就使用动态机制和现实信令进行接纳控制。可以看出，DiffServ区的路由器控制平面是RSVP而数据平面仍是DiffServ，这样既充分利用RSVP信令的优越性，又保持DiffServ的可扩展性。

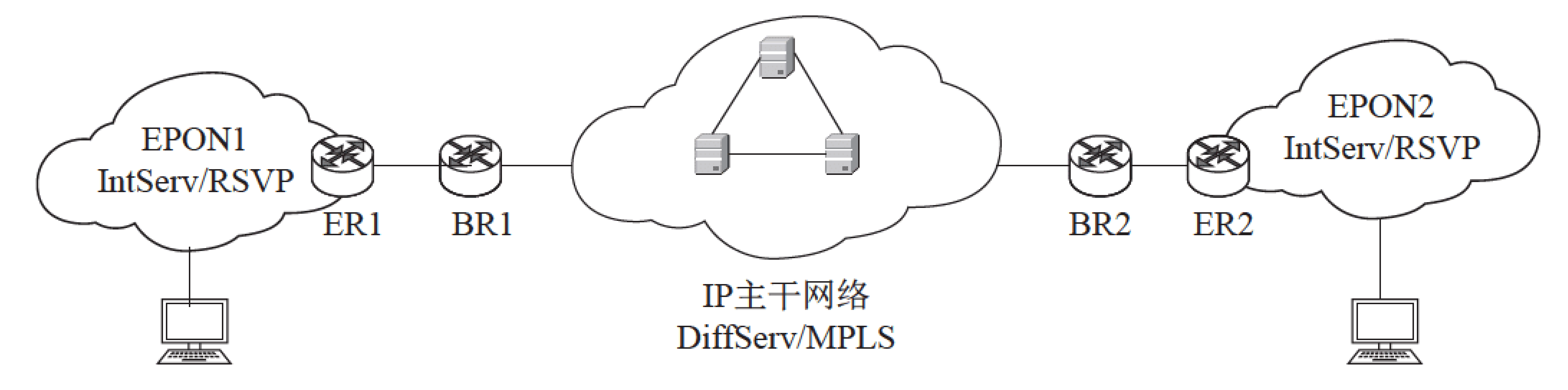


图5-10　IntServ模型和DiffServ模型的结合

2. 业务等级映射关系

1）IntServ中业务等级映射

在电力终端通信接入网中，采用IntServ模型来保障接入的QoS。为区分业务的等级，IntServ定义了三类服务，分别是确保服务、可控负载服务和尽力而为服务。上文已提到，确保服务和可控负载服务对QoS有相应的要求，尽力而为服务没有任何QoS保证。RFC2212定义了确保服务的特性，它必须为数据流提供端到端的有严格时延上限和低分组丢包率的服务。RFC211对可控负载服务进行了定义，它要求网络在任何时候都为其提供的服务能够达到“负载不重情况下网络所能提供的尽力”，网络负载过重情况下提供类似于网络低负载时所能提供的尽力而为服务。

基于IntServ服务类型的特点和智能配电网中业务等级及QoS需求，对智能配电网中的业务进行以下映射，参见表5-24。

表5-24　智能配电网通信业务等级到IntServ业务类型的映射

智能配电网通信业务等级	IntServ业务类型
紧急业务	确保业务
重点业务	可控负载服务
标准业务	
适度业务	尽力而为服务

① 紧急业务需要有保证的带宽和较高的时延要求，因此将此类业务映射为IntServ重的确保业务。

② 重点业务和标准业务对时延的要求较低，映射为可控负载业务。

③ 适度业务对时延的要求宽松，没有特别的QoS需求，因此映射成尽力而为的业务。

2）IntServ和DiffServ业务类型的映射

DiffServ区要能够为标准的IntServ的QoS服务提供支持，必须实现两个区的业务映射。将IntServ的确保服务在DiffServ中映射为EF PHB；IntServ中的可控负载服务在DiffServ中转换为AF PHB，而对于IntServ中的尽力而为业务在DiffServ网络中不给予QoS保证，仅采取尽力而为转发。映射结果如表5-25所示。

表5-25　IntServ和DiffServ业务类型映射

IntServ业务类型	DiffServ业务类型
确保业务	EF
可控负载业务	AFxy
尽力而为业务	BE

IntServ中的可控负载业务对应着智能配电网中的重点业务和标准业务，两类业务对QoS的需求是有差别的。在向DiffServ 映射的过程中，可控负载业务映射为AF业务，而AF业务包括AF1～AF4四类。因此，为了更加具体地区分各类业务，建立了以下映射机制：

① 紧急类业务映射为EF。通过将所有这些分组放置于一个专用的EF队列中，确保

EF数据包得到的服务速率高于数据包达到的速率。EF类的逐条行为策略能够提供低丢包率、低时延、低抖动和有保证的带宽服务。通过这种方式，使实时业务获得类似于租用线路的服务。

② 重点业务映射为AF3。为该级别的AF数据流量分配特定数量的转发资源（比如缓冲区和带宽），需要时，还可以进一步为每个分组指派不同丢弃优先级中的一种，如AF11、AF12或AF13。请注意，这些子类被放在同一个队列中。

③ 标准业务映射为AF2。该级别的业务允许有时延和缓冲，需要时也可以进行子类的划分。

④ 适度业务映射为BE。等价于尽力而为的默认模式。

⑤ 在EPON中，与静态带宽相比较，动态带宽分配更加灵活，能够更好地满足各业务的QoS要求。由于紧急业务、重点业务、标准业务、适度业务等电力通信业务的QoS需求不同，在使用EPON技术作为接入技术时，将使用不同的DBA模式。根据DBA模式的特点及电力通信业务的需求，对DBA模式和电力通信业务进行映射，如表5-26所示。

表5-26　DBA模式和电力通信业务的映射

模　式	定　义	电力通信业务
模式1	固定带宽	紧急业务
模式2	保证带宽	重点业务
模式3	保证带宽+最大带宽	标准业务
模式4	最大带宽	适度业务
模式5	固定带宽+保证带宽+最大带宽	

5.8.2　LTE的业务等级映射及QoS机制

1. LTE QoS机制的特点

QoS（服务质量）是指用户获得服务性能的总效果。从业务这一方面来说，QoS是由一些指标来衡量的，例如带宽、时延、丢包率等，不同的应用对QoS各项指标的要求不同。对于用户来说，用户对网络提供服务的满意程度越高意味着网络的QoS越高。

随着无线通信系统从2G、3G发展到如今的LTE/SAE，其QoS的实现机制也经历了一步步的演进过程。

在2G时代，因为语音是基于电路交换的，在进行数据传输之前首先得建立一条电路连接，一旦电路连接建立就能保证业务的服务质量，所以2G通信系统的QoS机制较为简单。对于被称作2.5G的GPRS，尽管其采用了分组交换的方式，但因其无线技术的限制，其对业务不能提供传输时延或者数据速率方面的保证，仅能提供尽力而为的服务。3G-UMTS定义了专用传输信道的概念，为了保持与专用信道定义的所有可能选项的一致性，不仅增加了一些新的QoS参数，还进一步细化了部分QoS参数，为已有的电路交换业务和新型的

分组交互业务提供了更加灵活的网络资源分配机制和调度策略。并且，其根据对时延的要求的不同，定义了会话类、交互类、流类、后台类四种QoS业务类型及其对应的具体QoS属性。发展到LTE/SAE，所用的QoS机制又做了一定的改进和简化。LTE/SAE采用了预定义的承载类型，确定了各类业务的不同QoS需求，带给用户高速流畅的体验：简化了属性域和标签的预定义，减少了可能的组合数量，从而减轻了网络的信令负荷；引入了默认承载，缩短业务建立时延，为用户提供“永远在线”的体验；保持不同设备商对同类型业务的服务质量一致性，实现用户跨网络的无缝移动体验。LTE的QoS机制有如下四个特点：

（1）基于网络的QoS控制

相比传统的QoS控制由UE侧发起，EPS承载的QoS控制策略的决策和下发均由网络侧决定，减少了QoS协商步骤，避免了网络资源的浪费，有效提高了网络资源利用率。

（2）简化QoS控制参数

将QoS的控制参数简化为4个参数，有利于业务QoS策略的制定和下发。

（3）提高资源复用能力

引入聚合最大带宽概念，对资源进行统筹管理，避免承载空闲态的预留资源浪费，提高承载的统计复用能力，提高了无线资源的使用效率。

（4）多级QoS控制力度

给出基于承载级、APN级、用户级三种力度的QoS控制机制，为制定更灵活的业务策略提供QoS保证。

2. EPS承载的业务架构

LTE系统中，QoS保障策略由网络侧决定，由终端、无线网eNodeB、核心网EPS设备共同实现。由于LTE系统中仅有共享信道，因此完全依靠QoS机制保障用户体验。EPS承载是QoS控制的最小粒度，所有映射到同一个EPS承载上的数据流都具有相同的QoS要求，也接受同等的数据包传输处理。

一般情况下，一个用户可以同时运行具有不同QoS要求的异类业务应用。例如，一个用户可以在浏览网页的同时进行VoIP通话。为了保障良好的用户体验，在LTE系统中，EPS内需要建立不同并且与特定服务质量QoS相关的EPS承载。换句话说，属于同一个EPS承载的所有业务默认具有相同的QoS等级，每一个EPS承载就代表一个不同的QoS等级。承载是QoS控制的基本粒度。对于EPS承载的概念，我们可以理解为UE与外部PDN之间的逻辑连接，这个逻辑连接的主要作用是为一个或多个SDF（业务数据流）提供传输基础。

与UMTS一样，LTE中的QoS承载业务架构也是划分层次和区域的。对于某一层，某一区域的承载，EPS都定义了明确的功能与属性，并且每一层的业务承载的实现都是由其接下来的一层承载所支持的。

如图5-11所示，EPS承载业务与外部承载业务共同提供了端到端业务。EPS承载的是核心网到终端的业务承载通道，在每个网元之间分段成一一对应的承载，即UE与EPC

之间的EPS承载由E-RAB提供，UE和eNodeB之间的EPS承载由Radio Bearer提供，Radio Bearer、E-RAB与EPS Bearer之间有一一对应关系。其中UE与eNodeB之间的业务承载功能为EPS无线承载，而EPS接入承载是指在eNodeB与MME之间的功能模块，这两个功能模块均不仅能提供业务数据的传送，还提供了业务QoS相关信息映射以及业务流分用复用等功能，共同组成了EPS承载。

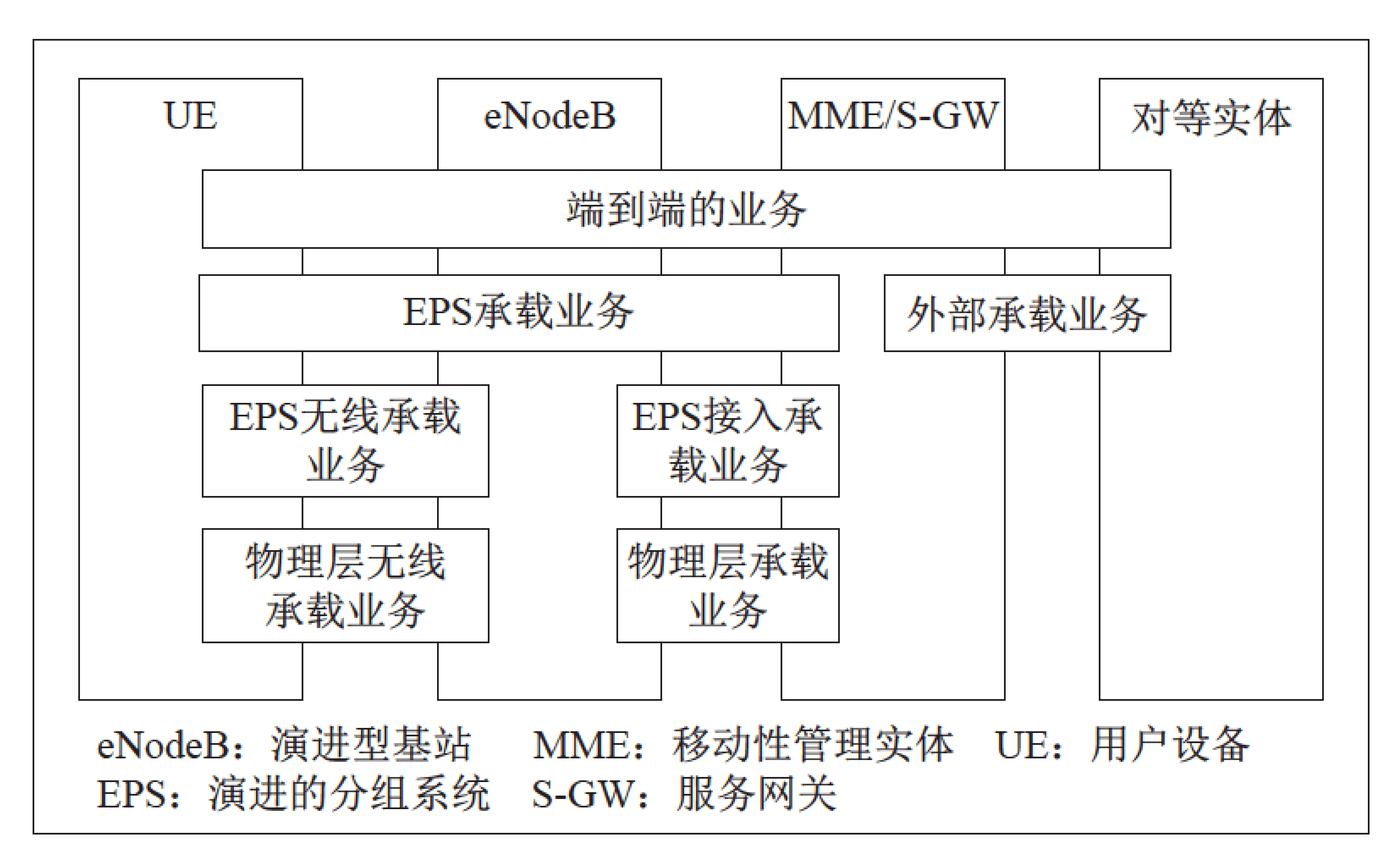


图5-11 EPS承载

EPS承载可以分为默认承载与专用承载。默认承载是为了给用户提供“永远在线”的体验而引入的，它提供一个尽力而为的逻辑连接，是一种支持满足默认QoS要求的数据和信令传输的承载。专用承载是为某些具有特定QoS要求所使用的，其相关的QoS参数一般要比默认QoS参数具有更高的优先级。

3. LTE中的QoS参数

LTE系统采用PCC架构，其中QoS参数由QoS authorization和QoS enforcement两个逻辑功能块产生和设置。QoS authorization功能在实体PCRF（Policy and Charging Rules Function）中实现，PCRF将基于业务应用层要求、用户签约信息和用户请求的QoS级别，根据PCC架构的策略进行综合评估，产生业务级的QoS参数。业务级的QoS参数包括QCI、ARP、GBR和MBR。

业务级的QoS参数与承载级的QoS参数映射在实体PCEF中完成，PCEF将对同一QoS参数的承载进行聚合，以便在核心网和无线网中统筹管理。承载级的QoS参数对于不同的业务类型，如GBR（保证比特速率）和Non-GBR（不保证比特速率）而有所不同，所有EPS Bearer都具有QoS Class Identifier（QCI）和Allocation and Retention Priority（ARP）这两个QoS参数。GBR业务中，为了保证速率，设置了Guaranteed Bit Rate（GBR）和Maximum Bit Rate（MBR）两个参数。对于Non-GBR业务，针对UE的每个APN设置Per APN Aggregate Maximum Bit Rate（APN-AMBR）参数，针对每个处于EMM-REGISTERED状

态的UE设置Per UE Aggregate Maximum Bit Rate（UE-AMR）参数。通常，承载级QoS分为GER和Non-GBR，具体参数包括：

GBR Bearer：QCI、ARP、GBR、MBR。

Non-GBR Bearer：QCI、ARP、APN-AMBR、UE-AMBR。

LTE系统中的QoS参数由核心网网元PCRF和PCEF产生，并通过S1接口传递到eNodeB，eNodeB在基站调度资源、接纳时都必须满足相应的业务QoS需求。除了APN-AMBR是MME和S-GW之间维护的参数以外，eNodeB中还会使用其他的QoS参数，包括QCI、ARP、GBR、MBR和UE-AMBR。

为了对各类QoS承载进行完整合理地描述，LTE系统定义了相关的几个参数，包括承载级、ARN级以及UE级，具体为：QCI（QoS Class Identifier）、ARP（Allocation/Retention Priority）、GBR（Guaranteed Bit Rate）、MBR（Maximum Bit Rate）和AMBR（Aggregate Maximum Bit Rate）。其中，AMBR可以分为基于ARN的AMBR和基于UE的AMBR。除了QCI和AMBR之外的其余参数均已在UMTS系统中定义。HSS可以存储与默认承载相关的签约QoS参数，而专用承载的QoS参数由P-GW动态生成。

QCI（QoS Class Identifier）是一个数量值，其标识这一个等级，描述了不同业务的QoS要求，包括业务类型、优先级、延时、丢包率等四项指标，是核心网根据业务特点和业务的无线需求进行设定的，主要用于调度优先级排序、调度、重传等机制中。目前协议中定义了1～9个标准QCI值，并规定可根据运营商需求扩展128～254的QCI值。可以由运营商根据实际需求在接入网节点（eNodeB）进行预配置。具有不同QCI值的承载具有不同的等级，在调度算法、接入控制算法等的处理也会有不同的优先级和门限值。QCI主要以保证各种业务的端到端的QoS需求为目标作用于承载建立后的资源调度控制，相较于UMTS的传输一套QoS参数，LTE使用QCI能够在保证不同设备间或者系统间的互联互通的能力下减少信令传输量，提高效率。

LTE网络中只传输QCI值，运营商可以根据需要在各网元中配置QCI与其他具体参数的对应关系，但依旧需要将标准取值作为基准，以保证在不同设备之间互通时QoS实现的一致性。对于每个SDF来说，其都有一个特定的QCI值，而具有相同的QCI与ARP值的多个SDF属于同一个集合。可以这样说，QCI代表了LTE系统为某个SDF提供的QoS特性。

表5-27描述了标准QCI属性。

表5-27　标准QCI属性

QCI	资源类型	优先级	数据包时延	丢包率	典型业务
1	GBR	2	100ms	10^{-2}	会话语音
2		4	150ms	10^{-3}	会话视频（直播流媒体）
3		3	50ms	10^{-3}	实时游戏
4		5	300ms	10^{-6}	非会话视频（缓冲流媒体）

续表

QCI	资源类型	优先级	数据包时延	丢包率	典型业务
5	NGBR	1	100ms	10^{-6}	IMS信令
6		7	100ms	10^{-3}	语音，视频（直播流媒体），交互式游戏
7		6	300ms	10^{-6}	视频（缓冲流媒体），基于TCP的业务（如WWW、E-mail、聊天、FTP、P2P文件共享等）
8		8			
9		9			

承载类型包括GBR承载和Non-GBR承载。承载类型决定业务是否被恒定地分配承载级别的资源。一个业务的承载类型由运营商配置策略决定，对于Non-GBR的SDF集合，只需静态策略与计费控制，而GBR的SDF集合需要动态的策略与计费控制。

优先级与QCI一一对应，用于区分不同SDF集合的服务等级，优先级值越小则服务等级越高。

在对分组数据进行处理和传输时，由于多数据包的抢占和竞赛，会出现数据包被延迟处理和传输的情况，分组时延预算表示了各个等级的SDF集合对于时延的容忍程度。

分组丢包率表示了各个等级的SDF集合对于数据传输丢包率容忍程度，它指的是非拥塞环境下的数据包丢失情况，具体为已在发送方ARQ处理但未成功到达对应接受方的数据包比率。此参数能够在链路层进行配置，并且同分组时延预算属性，能够支持对链路层相关功能尤其是调度功能的实现。

已建立的端到端的业务流一旦出现中断或者更新时，S-GW都会根据接收到相关信息对上述相关SDF集合以及集合描述做出更新。

最终，这个业务要落实到用户，还得需要S-GW将这个相关SDF集合描述发送给eNodeB，eNodeB据此来采取适当的调度策略进行无线资源管理。

ARP（Allocation and Retention Priority）包含业务承载优先级，抢占和被抢占标识，主要用于接纳和拥塞控制。在接纳时，基站将优先保证ARP优先级高的业务建立；当出现拥塞时，会根据业务的抢占标识决定是否去抢占现有业务的资源，根据被抢占标识决定是否被新建立业务抢占。由此可见，ARP只有在承载建立成功之前影响承载建立，一旦承载建立成功后，仅由其余四个参数决定承载的QoS等级。在新的承载发起新建或者已接入承载发起更新请求时，ARP可以根据资源当前的分配状态做出判决。在资源受限时，eNodeB还可以根据各个承载的ARP决定丢弃某个ARP等级较低的承载。ARP既可以用于GBR承载也可以用于Non-GBR承载。

对于GBR，顾名思义，其作用对象仅为GBR承载，为GBR承载提供保证的比特率。同GBR一样，MBR也仅作用于GBR承载，其值一般大于或等于GBR的值。它限制了GBR承载能够提供的最大的比特率。当业务的数据速率超过MBR时，系统将使用业务量整形算法来限制速率。

AMBR是针对EPS为了提高系统的带宽利用率引入的汇聚思想而定义的，可作为UE的签约参数保存在HSS中。同一个UE的多个Non-GBR承载可以共享相应某个AMBR的资源。特殊情况下，如果UE只有一个承载，那么这个仅有的承载就可以使用AMBR定义的全部带宽资源。同MBR一样，系统将在数据传输超过AMBR限制时使用业务流量整形算法进行调节。它是对某个APN相关联的所有承载进行累计比特率限制的，其实行实体上行为P-GW或UE，下行为P-GW。UE-AMBR的作用对象是UE，它的执行实体为eNodeB，相应的上下行UE-AMBR在UE与PDN之间建立起第一条IP连接时，通过默认承载建立流程传送给eNodeB。

GBR（Guaranteed Bit Rate）和MBR（Maximum Bit Rate）是GBR业务的特有参数，基站调度时会保证其传输速率。在现有协议中，GBR=MBR，即最大传输速率等于最小保障速率。

UE-AMBR（Per UE Aggregate Maximum Bit Rate）为UE聚合的最大传输速率，控制属于同一个UE的所有Non-GBR承载的数据速率的上限。即同一UE建立多个业务承载时，多个业务承载的传输速率总和必须不大于UE-AMBR，多余数据被丢弃，以保证UE之间的公平性。

4. LTE中的业务等级映射

在LTE网络中，QCI用来描述不同业务的QoS需求，可以由运营商根据实际需求在接入网节点（eNodeB）进行预配置。具有不同QCI值的承载具有不同的等级，对调度算法、接入控制算法等的处理也会有不同的优先级和门限值。QCI主要以保证各种业务的端到端的QoS需求为目标作用于承载建立后的资源调度控制，相较于UMTS的传输一套QoS参数，LTE使用QCI能够在保证不同设备间或者系统间的互联互通的能力下减少信令传输量，提高效率。

在同一个网络管理域中，应建立和维护一个一致的服务分类体系及相应的QoS行为定义。因此，应建立LTE网络中QCI到业务等级的映射，如表5-28所示。根据电力数据业务紧急业务、重点业务、标准业务以及适度业务对QoS的要求，将这四类业务与不同的QCI对应。紧急业务和重点业务需要有保证的带宽、低时延和低丢包率。由于GBR承载能够提供固定的传输资源，因此这两类业务采用GBR承载。而标准业务和适度业务对带宽、时延和丢包率的要求相对较低，故而采用Non-GBR承载。标准定义的QCI值1～9中，QCI=7，8，9时的丢包率、时延和业务类型完全一致，仅有优先级的区分。可见，针对同一业务，系统可以根据用户的不同，设置QCI=7，8，9。

EPC根据承载中的QoS信息，利用IP头中的TOS域中的8bit信息，分组包进行分类，不同的类别采用不同的分组转发方式。

表5-28 QCI与业务等级之间的映射关系

QCI	资源类型	优先级	电力数据业务
1	GBR	2	紧急业务
2		4	重点业务
3		3	紧急业务
4		5	重点业务
5	NGBR	1	—
6		7	标准业务
7		6	适度业务
8		8	
9		9	

5.9 终端通信网综合网络优化策略

现有的终端通信接入网包含了多种网络通信技术，形成大规模融合网络。引入终端通信接入网虚拟化技术，能够使该融合网络更好地提供通信业务服务以及充分利用通信网络资源。虚拟化是一种资源管理技术，是将计算机的各种实体资源，如服务器、网络、内存及存储等予以抽象、转换后呈现出来，打破实体结构间的不可切割的障碍，使用户能以比原本的组态更好的方式来应用这些资源。因此，虚拟化技术是终端通信接入网不可或缺的一部分。此处基于虚拟化的综合网络优化策略主要体现在以下几点（参见图5-12）。

① 进行底层物理网络的路由优化，整合底层物理网络资源，充分满足不同业务的需求，给出终端通信网络的路由优化策略。

② 将弹性资源配置方案嵌入虚拟网络全局控制器中，调配网络资源，优化资源管理结构。

③ 基于资源分配的跨域虚拟网络映射方案，以业务需求驱动虚拟网络映射，合理建立物理资源与虚拟网络节点、链路之间的映射关系，多域虚拟网络映射能够充分利用网络资源并进行网络资源隔离；同时提供一种面向流的虚拟网络调度方案，在虚拟网络集中控制以及资源状态信息透明的情况下，评估节点状态，流状态以及链路的状态，合理地调控流的传输。本节将主要讲述基于资源分配的跨域虚拟网络映射方案和面向流的虚拟网络调度方案。

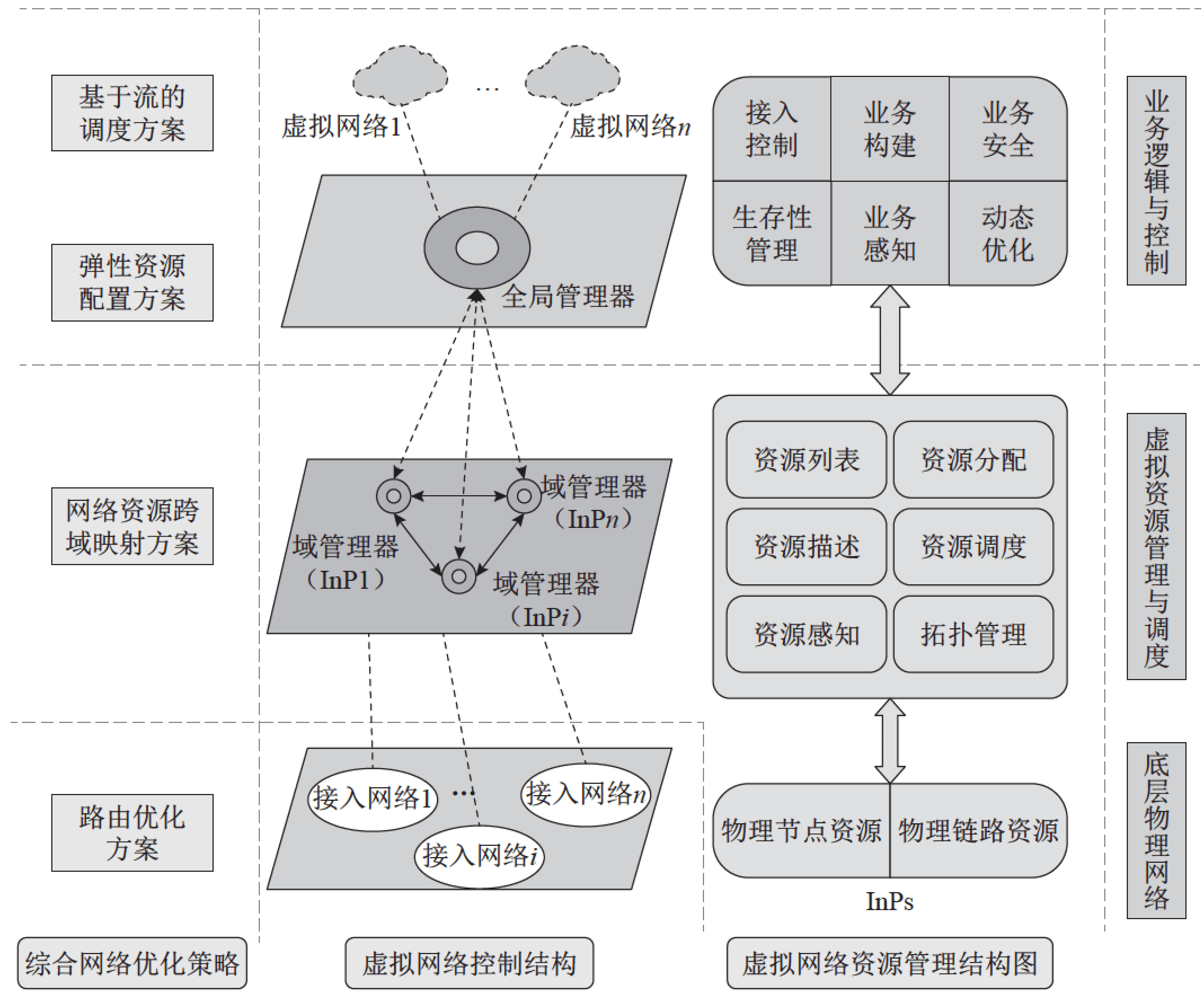


图5-12　基于虚拟化的综合网络优化策略

5.9.1　基于虚拟化技术的终端通信网络分层模型

虚拟化技术将物理资源转变为逻辑上可以管理的资源，打破了物理结构之间的壁垒，完成高层与底层之间的隔离。例如，虚拟层隐藏了下面的物理资源，用户可以不知道，但是可以使用；同时也可以隔离硬件和应用软件，如同他们属于不同的物理计算机，若其中一台虚拟机发生故障并不会影响其他操作系统，从而实现了故障隔离。终端通信网络类型复杂多样，有线网包括光纤网络、PLC网络等，无线网包括3G/4G网络、无线专网、Wi Fi等。面向类型复杂多样的终端通信接入网络，需要整合底层物理网络、物理资源，隔离网络类型的不同，完成网络差异化服务。基于此目的，一种基于网络虚拟化技术的终端接入通信网络架构被提出如图5-13所示。

基于网络虚拟化技术的终端接入通信网络架构由三层组成，基础设施层、虚拟化资源调度层、业务逻辑层。

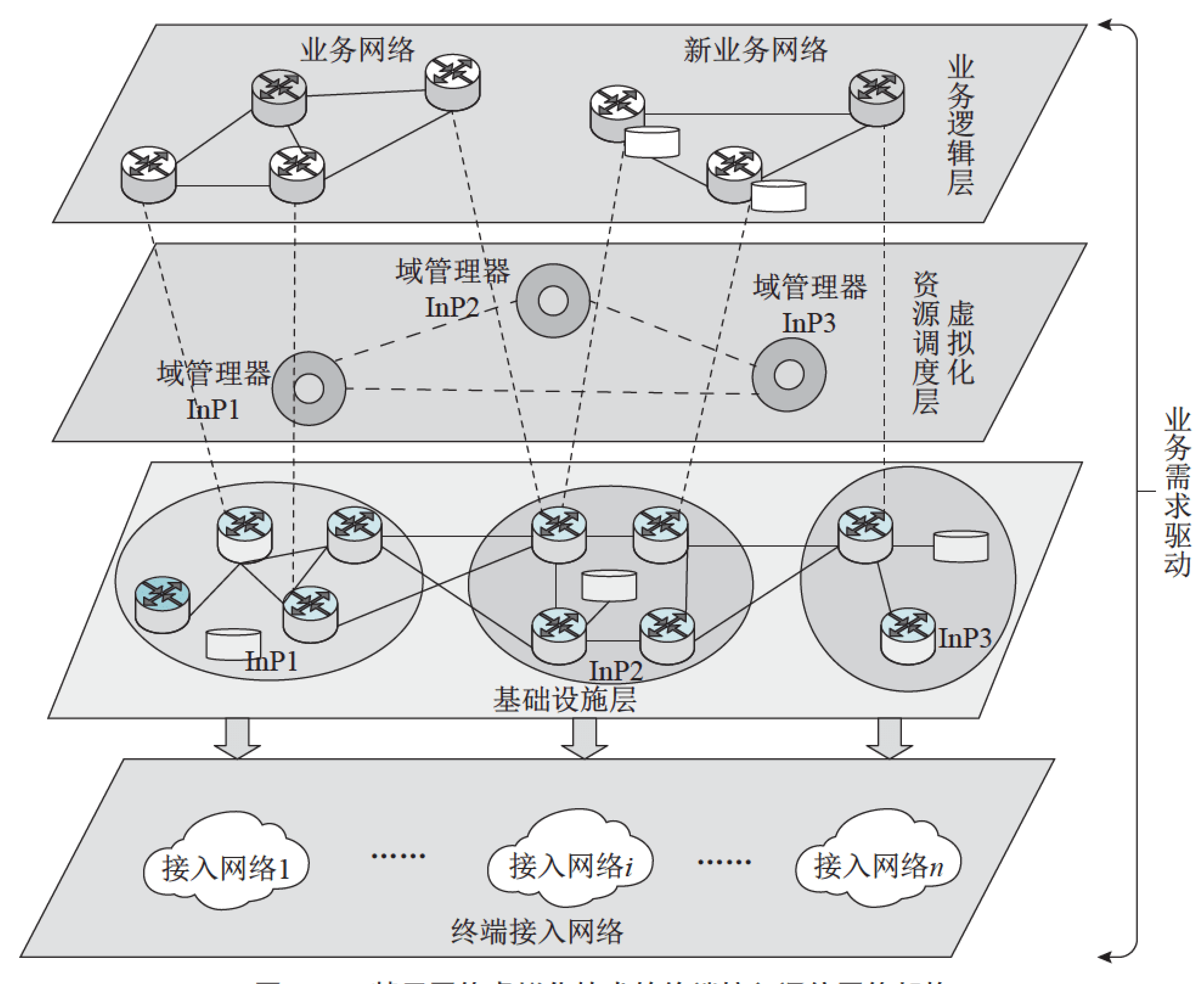


图5-13　基于网络虚拟化技术的终端接入通信网络架构

- 基础设施层：该层由众多基础设施提供者（Infrastructure Provider，InP）组成，每个InP表示一种类型的物理网络，比如工业以太网、GPON、PLC网络等。假设每个InP内的物理网络节点（交换机、路由器、ONU、边缘服务器等）都支持可编程功能和虚拟化功能，如InP通过虚拟化资源统一描述方式将底层物理资源的细节屏蔽，为上一层提供统一的虚拟资源抽象。
- 虚拟化资源调度层：该层基于分布式智能多域系统，基础设施层的每个InP将其物理资源抽象后组成一个域，每个域由一个域管理器进行虚拟资源管理。每个域管理器对应响应的一个InP，负责资源的探测和抽象、虚拟资源的分配和调度，以及虚拟网的创建和实例化。

管理器之间的协同和交互可以采用集中或分布式的方式，按照特定的协议交互信息，共享域管理器间的资源信息。每个域管理器内部由一系列相应的功能模块构成，包括资源发现、情景建模、资源映射以及特定的策略库等，如图5-14所示。

资源发现主要是确定其网络管理的拓扑和相应网络元素的状态，更进一步，邻近的域管理器也同样共享状态信息，在网络之间建立链路实现域间虚拟网络的构建。虚拟资源映射主要是按照策略库中的约束将虚拟化节点和虚拟化链路分配到相应的物理节点和路径上。

可获得资源列表
情境建模
信息获取
映射
策略库

可获得资源列表
情境建模
信息获取
映射
策略库

可获得资源列表
情境建模
信息获取
映射
策略库

图5-14　域管理器之间的交互

- 业务逻辑层：该层由众多的相互隔离的虚拟网络组成，这些虚拟网由用户或者用户代理发起的请求驱动，由域管理器进行调度、分配和创建完成特定的功能。

5.9.2　网络资源映射算法

1. 物理网络系统抽象描述

底层基础设施由无向图 $G_s=(V_s,E_s)$ 表示，其中V_s和E_s分别是物理节点集合和物理链路集合。G_s由n个InP所管理的域通过域间链路互联构成。第 k 个InP所管理的域定义为 $G_{s,k}=(V_{s,k},E_{s,k})$，其中$V_{s,k}$和$E_{s,k}$分别是域内的物理节点集合和物理链路集合。定义域间物理链路集合为$E_{s,I}$。那么，G_s即为 $G_s=G_{s,1}\cup G_{s,2}\cup\cdots\cup G_{s,N}\cup E_{s,I}$。其中$V_s$为 $V_s=V_{s,1}\cup V_{s,2}\cup\cdots\cup V_{s,N}$，且 E_s 为 $E_s=E_{s,1}\cup E_{s,2}\cup\cdots\cup E_{s,N}\cup E_{s,I}$。图5-15所示的底层基础设施由三个域和域间链路组成。

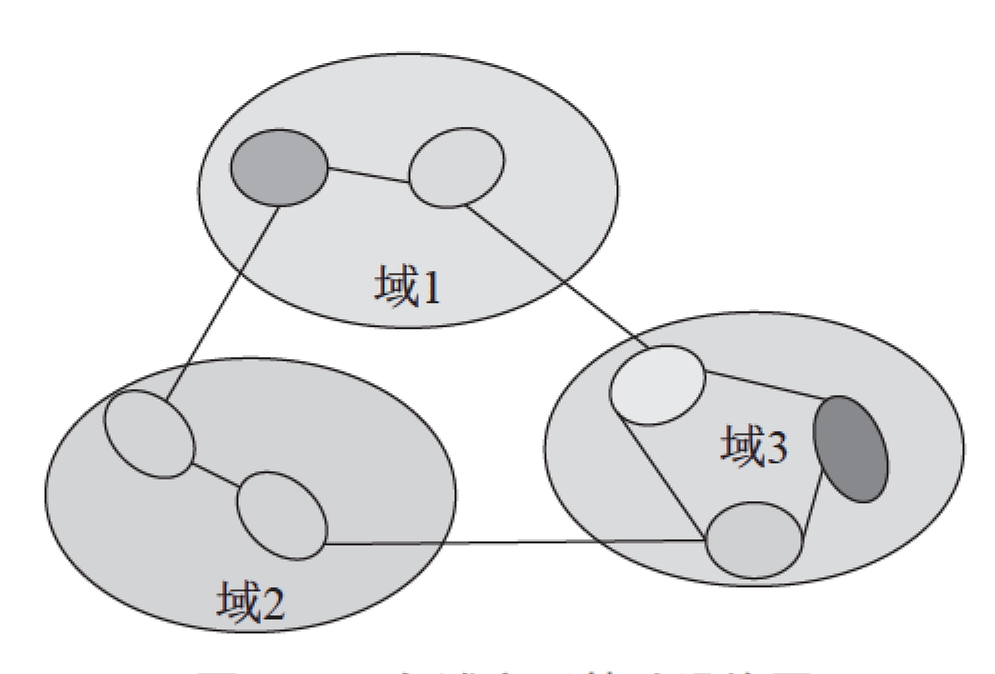


图5-15　多域底层基础设施图

物理节点 $n_s \in V_s$ 上的可用网络资源（如带宽）定义为 $C_s(n_s)$。一条物理链路定义为 $l_s=(s,t)\in E_s$，其中，s和t为物理链路的两个端点。物理链路l_s上的可用带宽定义为$B_s(l_s)$。在单域环境下，资源管理者和映射的决策者通常是同一个角色，因此资源消耗对其来说是"成本"，而跨域的映射环境下，全局映射的决策者和域内资源的管理者是不同角色，如图5-16所示。因此资源的消耗对于全局决策者来说是"价格"。此处，假设"成本"与"价格"是相同的，那么在竞价机制下，InP域内的映射成本就是给全局映射决策者的报价。物理节点ns上的单位计算容量价格（成本）定义为$u_N(n_s)$。物理链路l_s上的单位带宽价格（成本）定义为$u_L(l_s)$。另外物理链路上的时延定义为$d(l)$。

2. 虚拟节点请求

虚拟节点（Virtual Node，VN）请求由无向图 $G_V=(V_V,E_V)$ 表示，其中V_V和E_V分别是虚拟节点集合和虚拟链路集合。对于一个虚拟节点 $n_V \in V_V$，此虚拟节点所需要的计算资源为 $C_V(n_V)$。一条虚拟链路定义为 l_V 所需的带宽定义为 $B_V(l_V)$。因为节点映射会涉及具有地理位置的要求，故设放置虚拟节点n_V的物理节点的集合为 $L(n_V)$。

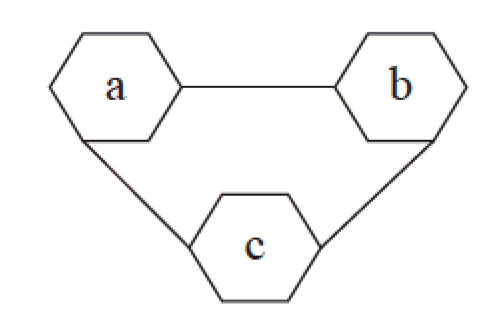


图5-16　虚拟节点请求

3. 虚拟节点跨域资源分配

1）全局映射视角

在满足一定约束条件下虚拟节点和虚拟链路映射到物理节点和物理链路上。虚拟节点n_V映射在物理节点n_s上的节点映射定义如下：

$$n_V \to n_s : M(n_V)=n_s \ , n_V \in V_V, n_s \in V_s \tag{5-7}$$

节点映射的资源约束和映射分离约束为：

$$\begin{aligned} &C_s(M(n_V)) \geqslant C_s(n_V), \forall n_V \in V_V \\ &M(i)\neq M(j), \forall i,j \in V_V \text{且} i\neq j \end{aligned} \tag{5-8}$$

且节点映射还需要满足虚拟节点可行映射区域要求，约束如下：

$$M(n_V)\in L(n_V) \ , \forall n_V \in V_V \tag{5-9}$$

在底层基础设施G_s上，两个不同的物理节点s和t之间的物理路径集合定义为$P(s,t)$。此处不考虑链路分割，因此虚拟链路 $l_V=(i,j)$ 映射在路径 $p(l_V)$ 上的链路映射定义如下：

$$l_V=(i,j)\rightarrow p(l_V):M(l_V)=p\quad ,l_V\in E_V,p(l_V)\in P(M(i),M(j)) \tag{5-10}$$

链路映射的带宽资源约束如下：

$$B_s(l_s)\geqslant\sum_{p:l_s\in P}B(l_y)\ ,\forall l_V\in E_V \tag{5-11}$$

此外，虚拟链路 l_V 的时延 $d_V(l_V)$ 为其所映射至物理路径的时延，定义如下：

$$d_V(l_V)=\sum_{l_s\in p(l_V)}d(l_s)\ ,\forall l_V\in E_V \tag{5-12}$$

2）分布式映射视角

上文以全局的角度描述了跨域VN映射，由于InP对外不公开所管理的域内具体的拓扑和资源信息，VN映射的决策者只决定虚拟节点和虚拟链路的放置在哪个域之中，域内具体映射由InP完成。

在映射决策者所进行的域级映射中，虚拟节点 $n_V\in V_V$ 映射到域 $G_{S,k}$ 中表示为 $D(n_V)=k$，具体定义如下：

$$n_V\rightarrow G_{S,k}:D(n_V)=k\ ,n_V\in V_V,G_{S,k}\subseteq G_S \tag{5-13}$$

虚拟链路 $l_V\in E_V$ 映射到域 $G_{S,k}$ 中，表示为

$$l_V\rightarrow G_{S,k}:D(l_V)=k\ ,l_V\in V_V,G_{S,k}\subseteq G_S \tag{5-14}$$

此外，若虚拟链路的两个顶点映射到不同的域中时，虚拟链路将经过域间链路。

如图5-17所示，跨域映射是映射决策者将图中的VN映射到对应的底层基础设施上。虚拟节点a映射在域2中，且虚拟节点b，c映射在域3中，同时虚拟链路（b，c）也映射在域2之中在域2与域3之间存在跨域的虚拟链路。

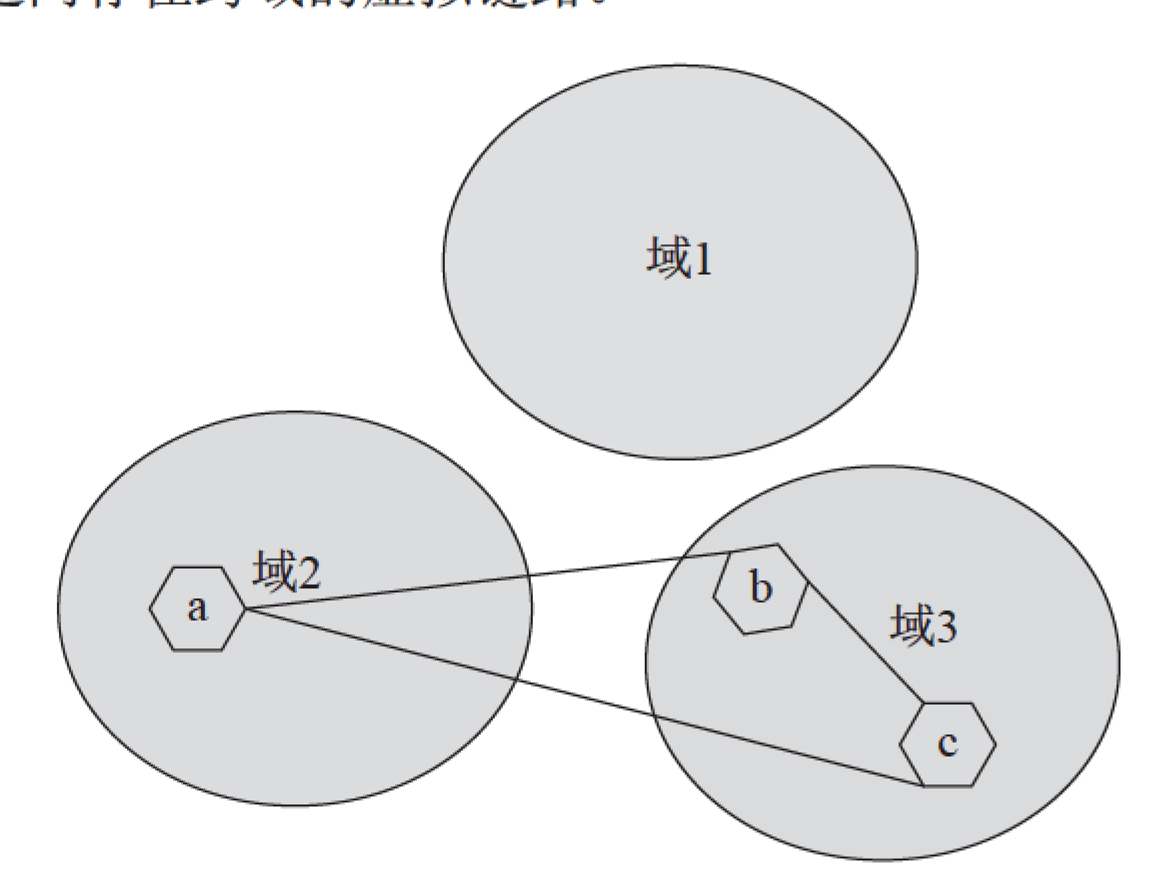


图5-17　域级映射

基于域级映射，VN被分成多个子图，每个子图映射在不同的域中。域内映射由InP完成，且这些域内映射就是单域问题。基于域级的VN映射只包含节点a和包含节点b、c以及链路 (b,c) 的子图，这两个子图的域内映射如图5-18所示。

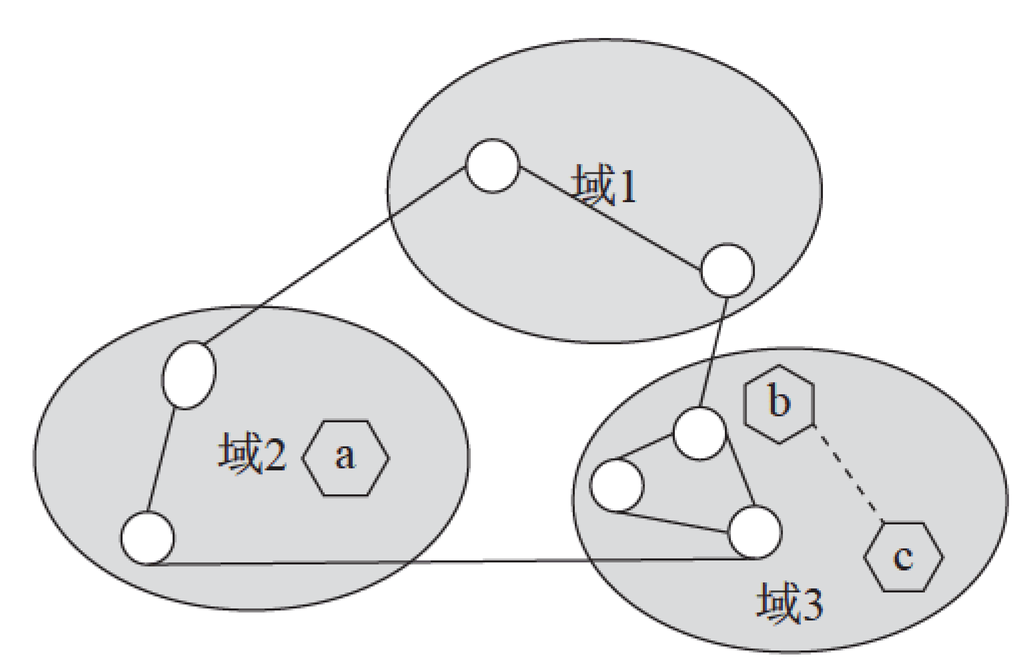


图5-18　域内映射

4. 跨域资源分配的效用函数

考虑到VN映射的全局映射价格和服务质量，并通过一个效用函数f来表达，同上文所述，将VN的全局价格定义为整个底层基础设施所分配资源的价格。虚拟节点$n_V \in V_V$的映射价格$f_N(n_V)$定义如下：

$$f_N(n_V) = u_N(M(n_V))C_V(n_V) \tag{5-15}$$

虚拟链路$l_V \in E_V$的映射价格定义为：

$$f_L(l_V) = \sum_{l_S \in p(l_V)} u_L(l_S)B_V(l_V) \tag{5-16}$$

则定义VN映射的总价格f_P为：

$$f_P = \sum_{l_V \in E_V} f_L(l_V) + \sum_{n_V \in N_V} f_N(n_V) \tag{5-17}$$

同时考虑到全局映射的服务质量表现，即所有虚拟链路最大时延$d_{\max}$，具体定义为：

$$d_{\max} = \max_{v \in E_V} d(l_V) \tag{5-18}$$

则映射效用函数定义为：

$$f = f_P + \alpha d_{\max} \tag{5-19}$$

式（5-19）中的α表示$d_{\max}$的重要程度，且用来保障f_P和$d_{\max}$的数值在同一数量级。对于全局映射的决策者，效用函数越小越好。

5. 虚拟节点的跨域资源分配机制

全局映射决策者的问题是在不知道各个域内信息的条件下决定虚拟节点和虚拟链路的域级映射以及最小化映射函数f。针对各个InP，类似于单域映射问题，它的问题是最小化映射价格。在此以MD-VNM来解决上述问题。

1）域内候选资源的提供

采用单域映射算法Improved-vnmFlib的思路来寻找候选映射，由于域内选择映射

时VN并非映射到整个域内，所以对Improved-vnmFlib进行简化和修改，以用在域内寻找低价格的候选映射。算法在寻找低价格的候选映射时，其节点候选映射信息设为：$Cad_{N,k}\left(n_V,f_N\left(n_V\right)\right)$。在算法内部定义集合$T$记录所有尝试过映射的虚拟节点，集合$M$记录所有成功映射的虚拟节点，而$S$集合记录候选映射信息作为算法的输出结果。算法步骤如下：

输入：VN请求(V_V,E_V)，单域底层基础设施$(V_{S,k},E_{S,k})(1\leqslant k\leqslant N)$。

功能：在$(V_{S,k},E_{S,k})$上为(V_V,E_V)寻找价格最低的候选映射。

输出：候选映射集合S。

步骤1　$T=\phi,M=\phi,S=\phi$。

步骤2　从V_V中选择与M中虚拟节点有联系的虚拟节点$n_V(n_V\in M)$。若$M=\phi$，n_V则直接从V_V中选择。

步骤3　遍历域内的物理节点，寻找最小化n_V和$\{l_V=(i,n_V)\in E_V\ /\ i\in M\}$。映射价格的可映射（满足约束条件的）物理节点及相关物理路径。

步骤4　若n_V和$\{l_V=(i,n_V)\in E_V\ /\ i\in M\}$存在可行映射，则以找到的可行映射更新资源信息，并将n_V放入集合M中。将n_V和$\{l_V=(i,n_V)\in E_V\ /\ i\in M\}$的候选信息放入$S$中。

步骤5　将n_V放入集合T中。

步骤6　若所有的虚拟节点都尝试过映射$(|T|=|V_V|)$，算法完成并输出S，否则，回到步骤2。

算法的步骤3中链路的映射采用Dijkstra算法逐一为相关的虚拟链路寻找满足带宽需求的最低价格路径。

2）多域辅助图的构建

映射管理器收集来自不同InP的候选映射，构建全局图。全局图的构建分为两步：将每个InP提供的候选节点和链路加入到全局图中；为不同InP的候选节点之间按照VN中的虚拟链路增加跨域候选链路。全局图包括了InP提供的域内的链路候选映射和跨域的链路候选映射（虚线表示）。

全局图由无向图$G_D(V_D,E_D)$表示，其中V_D和E_D分别为候选节点和候选链路的集合。定义由$CF_N\left(n_D\right)=n_V$表示候选节点$n_D\in V_D$是虚拟节点n_V的映射候选。并且n_D的价格定义为$pc_N(n_D)$。定义由$CF_L(l_D)=l_V$表示候选链路$l_D\in E_D$时虚拟链路l_V的映射候选，其中，$l_D=(i,j)$，$l_V=(CF_N(i),CF_N(j))$且l_D的价格和时延分别定义为$pc_L(l_D)$和$d_D(l_D)$。其中候选映射的信息都由InP提供。全局图构建的具体步骤如下：

输入：所有InP的候选信息。

功能：构建全局图(V_D,E_D)。

输出：全局图(V_D,E_D)。

步骤1 $V_D=\phi, E_D=\phi, i=1$。

步骤2 选择第 i 个InP。

步骤3 按照InP提供的所有节点映射候选信息 $Cad_{N,k}(n_V, f_N(n_V))$，$CF_N(n_D)=n_V$ 和 $pc_N(n_D)=f_N(n_V)$ 和链路映射候选信息 $Cad_{L,i}(l_V, f_l(l_V), d_V(l_V))$，$(CF_L(l_D)=l_V, pc_L(l_D)=f_L(l_V), d_D(l_D)=d_V(l_V))$ 建立候选节点n_D和候选链路l_D，并分别加入V_D和E_D中。

步骤4 若i小于N，则回到步骤2。

步骤5 逐一从所有候选节点对 $\{(m,n)或(n,m)/\forall m,n\in V_D, m\neq n\}$ 进行选择；如果遍历完成，算法结束。

步骤6 如果 $(CF_N(m), CF_N(m))\in E_V$，继续步骤5。

步骤7 为 (m,n) 选择一条满足虚拟链路 $(CF_N(m), CF_N(m))$ 带宽需求的最低价格跨域路径p。

步骤8 按照跨域路径 p 的价格 $price$ 和时延 $delay$ 建立链路候选 $l_D=(m,n)\big(CF_L(l_D)=(CF_N(m), CF_N(m)), pc_L(l_D)=price, d_D(l_D)=delay\big)$ 继续步骤5。

算法中步骤1到步骤4将所有的InP提供的候选映射加入到全局图中，步骤5到步骤8则是为不同InP提供候选节点之间建立跨域候选链路。步骤7中的 m 和 n 必定对应不同的InP，因为域内两个虚拟节点提供映射的同时也必须为两点之间的虚拟链路提供候选映射。跨域路径的选择由所有的InP和管理器协同完成。每个InP提供域内源目的节点之间的（满足带宽需求的）路段信息，如价格和时延，并提供映射管理器，UN管理器再从路段中组合出最低价格路径。具体的实现是将所有的路段作为由边组成的拓扑，并在该拓扑上采用Dijkstra算法，即可找到最低价格路径。

3）跨域资源的选择

在构建完全局图后，映射管理器在其上选择候选映射以完成VN的跨域映射。候选映射的选择以最小化式（5-13）的效用函数为目标，用候选映射的选择建立MILP模型，并采用整数松弛算法求解。

（1）MILP模型

变量定义：

定义 $x(n_D)$ 为 $0\sim1$ 的整数变量，若候选节点n_D被选中则为1，否则为0；定义 $y(l_D)$。

同样为 $0\sim1$ 的整数变量，若候选链路l_D被选中则为1，否则为0；定义$d_{\max}$为连续变量，所有选中的候选链路中的最大时延。候选映射选择的MILP模型如下：

目标函数：

$$\min\sum_{n_D\in V_D} x(n_D)\, pc_N(n_D)+\sum_{l_D\in E_D} y(l_D) pc_L(l_D)+\alpha d_{\max} \tag{5-20}$$

约束条件：

$$\sum_{n_D:CF_N(n_D)=n_V} x(n_D)=1,\forall n_V=V_V \tag{5-21}$$

$$\sum_{l_D:CF_L(l_D)=l_V} y(l_D)=1,\forall l_V\in E_V \tag{5-22}$$

$$x(n_D)\geqslant y(l_D),\forall l_D=(n_D,j)\in E_D \tag{5-23}$$
$$x(n_D)\geqslant y(l_D),\forall l_D=(I,n_D)\in E_D$$

$$d_{\max}\geqslant d_D(l_D)y(l_D),\forall l_D\in E_D \tag{5-24}$$

$$x(n_D)\in\{0,1\},\ \forall n_D\in V_D \tag{5-25}$$

$$y(l_D)\in\{0,1\},\quad \forall l_D\in E_D \tag{5-26}$$

目标函数式（5-20）和最小化式定义的映射效用函数，包括映射价格和虚拟链路最大时延。约束式（5-21）到式（5-26）是可行性约束，保证选择的候选映射可以组成整个VN映射。约束式（5-21）和式（5-22）保证VN请求中的所有虚拟节点和虚拟链路都选择了一个候选映射与之对应。约束式（5-23）和式（5-24）保证了当一个候选链路被选中时，其端点（候选节点）也同时被选中。约束式（5-25）和式（5-26）用于记录所有$x(n_D)$和$y(l_D)$是0～1整数变量及$d_{\max}$时连续变量。

（2）整数松弛方法

由于候选映射选择问题是NP的难题，因此需要提出一个启发式算法。本节采用整数松弛方法求解上述模型。候选映射选择模型整数松弛的步骤如下：

输入：候选映射选择整数规划模型。

功能：以最小化价格目标寻找候选映射。

输出：选中的候选映射集合F，即跨域VN映射结果。

步骤1　令$F=\phi$。

步骤2　将模型中的变量$x(n_D),\forall n_D\in V_D$和$y(l_D),\forall l_D\in E_D$松弛为0～1的连续变量。

步骤3　求解松弛后的线性规划模型，求得松弛后的$x(n_D),\forall n_D\in V_D$和$y(l_D),\forall l_D\in E_D$的解。

步骤4　遍历所有虚拟节点$n_V\in V_V$，为每个n_V选择从所有的对应的候选节点$CF_N(n_D)=n_V$中选择$x(n_D)$最大的n_D，即$n_D=arg\max\limits_{n_D:CF_N(n_D)=n_V} x(n_D)$，并放入集合$F$中。

步骤5　选择所有虚拟节点之间的候选链路，即将$\{l_D=(i,j)\in E_D/\forall i,j\in F,(CF_N(i),CF_N(j))\in V_D\}$放入集合$F$中。

在全局图中，如果任意两个候选节点对应的虚拟节点之间存在虚拟链路，那么这两个候选节点之间必然存在对应的候选链路。因此，基于模型松弛后的解，只需要确定候选节

点就可以确定全部的候选映射。选中的候选映射就是VN的跨域映射。

5.9.3 面向流的虚拟网络调度方案

如图5-19所示，传统的最短路径算法往往会导致网络节点过载，图（a）显示一些节点已经有些负载。图（b）有新流*A*→*D*申请产生，在节点间有三条可选路径：*AEFGD*、*AGD*和*ABCD*。通过传统最短路径算法计算得到路径*AGD*，但此时*A*、*G*点都存在负载，因此可能引起节点超载。图（c）通过收集三条路径实时运行状态，得出最优路径*ABCD*。这些运行状态是实时的，因此实现算法也必须是实时的。

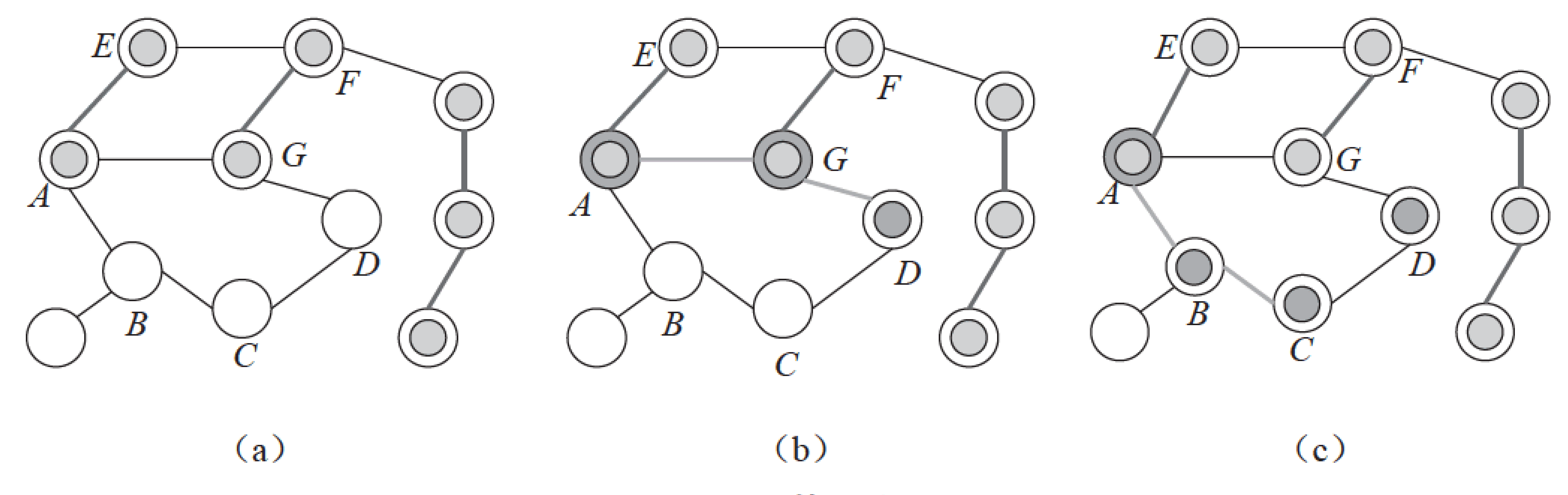


图5-19　算法流程

如果网络无法知晓全局的资源利用率情况，不能做到负载转移分流，这样就不能充分利用网路中的资源，导致网络资源利用率降低。如图5-20所示，图（a）显示在某初始环境下，网络中有三个流*A*→*E*、*A*→*F*、*A*→*D*，分别承载的节点路径为*AE*、*AGF*、*ABCD*。各节点创建本节点阈值来评价继续增加负载的能力，倾向性选择负载比较小的流，这样能够使得承载该服务后不超过阈值。系统某时刻需要创建新的流*A*→*D*，假设在评价体系下，流*A*→*D*负载很大。在独立节点情况下，各个节点不考虑全局信息，只根据本节点运行状态创建本节点阈值，如图（a）所示。*A*相邻结点*E*、*G*、*B*因节点本身独立阈值设置，均不能负载该流，系统拒绝承载该服务。如图（b）所示，在因控制器知悉全局情况下，控制器可调整*E*节点分流，流*A*→*F*改变路径为*AEF*，这样*G*节点因空出流*A*→*F*的承载能力，可以承载流*A*→*D*的服务，创建路径*AGD*。这种调度方式在路由器没有全局实时智能下不会出现，通常做法是拒绝服务造成丢包。图（c）是另外一种分配方式，将*ABCD*上的流段移到*AGD*，新建流以*ABCD*路径进行传输。控制器可根据一些权值判定哪种方式更加合理，再具体进行部署。

虚拟网络中域管理器以及全局控制器能够获得网络节点和链路的实时信息，这些信息具有全局性，虚拟网络环境能够充分满足本算法的特性，实现流的合理调度。

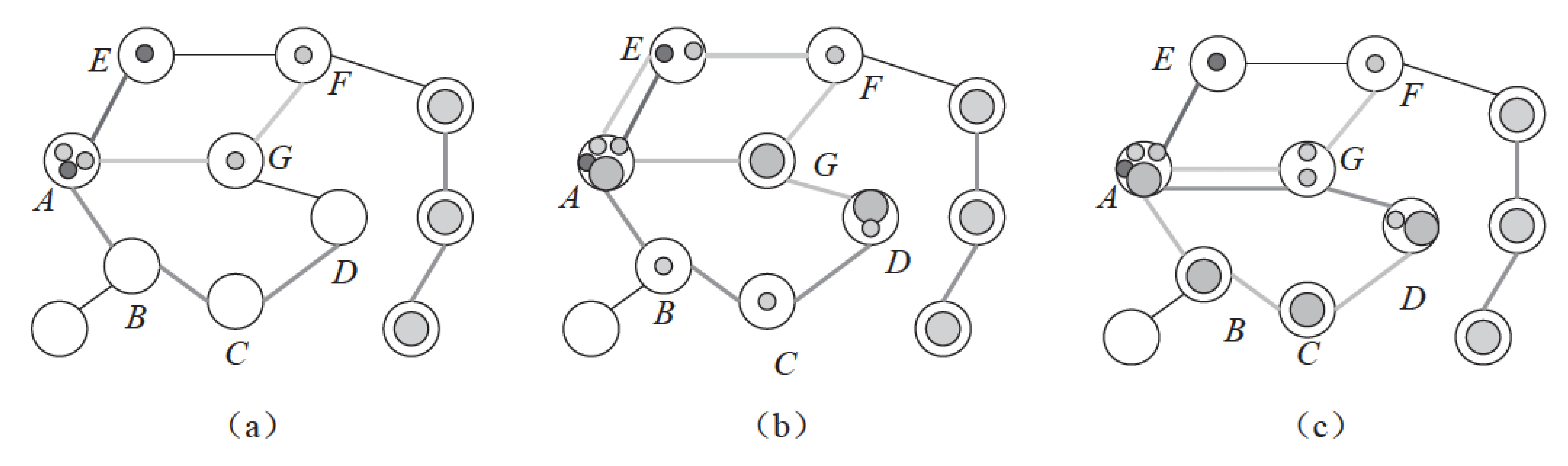


图5-20 算法流程

1. 节点评估

当交换节点负载超过阈值后，控制器需要对该节点上的流进行重新调度，减轻该节点负载。对于选出来的流，需要对其进行重新寻找路径算法操作。触发该算法事件是一个流需要重新放置时或者产生新的流。传统OSPF协议运行最短路径算法，对节点评估权值为$[Metric/b(S)]$。该算法有两个问题：

一是节点样本量过大。最短路径算法基本通过Dijkstra算法实现，此算法的时间复杂度为$O(n^2)$，n为节点个数。当没有采取启发性时，网络节点探测方式是圆形波阵面展开的，当节点数量很多时，算法消耗过大。有一些基于Dijkstra优化的算法，方式是对样本节点进行预优化，这样可以使选择样本减少，目前认为最好能够到$O(l+n\log(n))$，l为链接个数。

二是节点带宽不能反映当前节点运行时状态。传统算法中没有根据实际节点实际运行时情况，$b(S)$越大的节点，被分配的流越多，实际上越拥堵，所以需要对节点进行运行状态评估。节点评估算法可对当前节点可承载状态进行评估，路径选择算法可淘汰大量不在阈值范围内的节点以减少样本量，因此使用这两种算法能够有效解决传统算法的两个问题。采用节点评估算法需要在虚拟网络的全局控制模拟器中增加全局监控模块、独立动态计算模块，以及矩阵维护模块。

1）节点剩余带宽评估

节点剩余带宽评估（Node Left Bandwidth Evaluation，NLBE）方式为：

设节点S可被调用的带宽为$Avail(S)$，上限阈值为$TH^u(S)$，一般的有：

$$P_{w1}(S)\leqslant TH^u(S) \quad (5\text{-}27)$$

则剩余带宽为：

$$l(S)=b(S)-wl(S) \quad (5\text{-}28)$$

可被调用带宽为：

$$Avail(S)=TH^u(S)b(S)-wl(S) \quad (5\text{-}29)$$

拓扑中节点集合S中各节点状态 $b(S)$， b_{X_i} 为实际观测值，通过信息收集模块收集，并得到节点状态向量。 $wl(S)$、 $TH^u(S)$、 $Avail(S)$ 通过计算模块读取节点状态向量矩阵得到，并写到节点状态向量对应区域。路径算法读取 $Avail(S)$ 作为权值，淘汰大量不在阈值 $TH_{Avail(S)}$ 范围内的节点（本节算法为小于阈值情况），计算得出预测最优路径。其中，

$$TH_{Avail(S)} = \sum_{X_i \in X_{triqqer}} b_{X_i} \tag{5-30}$$

$X_{triqqer}$ 为触发最短路径算法发生时刻节点S同时新生成的流集合，一般情况下为了降低算法复杂度和增加即时反应速度，取静态经验值。

2）节点剩余流量评估

NLBE算法是基于节点本身的当前承载能力的，但是流频率 λ_{X_i} 没有被考虑， $\lambda_{X_i} b_{X_i}$ 流量传输特性对未来某节点运行状态有很大影响。假设某个时刻系统检测到一个带宽大的流正在运行，算得 $Avail(S)$ 值比较小，但其发生频率很小，之后便很少出现，这样会使得这段时间内实际 $Avail^{ac}(S)$ 值远大于计算 $Avail(S)$，造成资源浪费。同样情况，如果流带宽小但频率大，实际 $Avail^{ac}(S)$ 值远小于计算 $Avail(S)$，造成系统资源最优分配失败率增加。以上两种情况都会造成系统次优状态运行概率增加，整个系统处理能力降低。

节点剩余流量评估（Node Left Flux Evaluation，NLFE）方式为：记节点S可用流量为 $Flux_{Avail}(S)$，工作负载可记为：

$$wl_{F1}(S) = \sum_{i=1}^{n} b_{X_i} \lambda_{X_i} \tag{5-31}$$

流可能消失而造成剩下的流量为： $\sum_{i=1}^{n} b_{X_i}(1-\lambda_{X_i})$

可被调用流量为：

$$\begin{aligned} Flux_{Avail}(S) &= TH_F^u(S)b(S) + \sum_{i=1}^{n} b_{X_i}(1-\lambda_{X_i}) - wl_{F1}(S) \\ &= TH_F^u(S)b(S) + \sum_{i=1}^{n} b_{X_i}(1-2\lambda_{X_i}) \end{aligned} \tag{5-32}$$

由 $Flux_{Avail}(S)$ 定义可得到一些现象：当 $\lambda_{X_i}=1$ 时，该算法退化到NLBE算法。该流发生频率 $\lambda_{X_i}=1$ 时，可取固定预估值。当流带宽比价平稳，所有的流频率 $\lambda_{X_i} \leqslant 1/2$ 时，可知一定有足够的容纳带宽不超过阈值的流，这类节点被当作优质节点。最短路径算法选择节点时优先考虑优质节点，这样能够尽量缩短寻找节点时间。

2. 可选路径评估

可选路径评估法运用于新建流或者选出一些流后重新放置路径，此算法需要额外模

块。在某时刻T_i通过最短路径算法选出的节点状态是时刻T_i的状态，NLFE中通过流估计值λ_{X_i}来预估节点未来状态。鉴于控制器控制层面可扩展特性，可以建立两节点间的路径数据库，实时算法通过可选路径上节点状态来评估路径情况。当网络拓扑改变时，触发寻找两点路径集合算法，更新各网络路径数据库，该数据库仅记录两节点连通情况，非运行状态的复杂信息。运行状态信息收集模块收集各节点运行时信息，当发现某条路径上的一些节点超载时，排除这些路径，在剩下的可选路径中，通过下面的评价算法通过获取信息判定可选最优路径。

1）路径带宽评估

路径带宽评估（Link Bandwidth Evaluation，LBE）方式为：设路径集合开始节点S_{sour}和结束节点S_{des}表示为：$Path(S_{\text{sour}},S_{\text{des}})$为两节点可选路径集合，$P_i$为可选路径集合某一条路径，$S_{i,j}$为$P_i$路径上的某一传输节点。则$P_i$路径可用带宽为每条路径上节点带宽最小值决定，即有：

$$b_{P_i}=\left\{\min b_{S_{i,j}} \mid \forall S_{i,j}\in P_i\right\} \tag{5-33}$$

路径选择算法选择带宽最大的路径，即：

$$P_m=\left\{\max b_{P_i} \mid \forall P_i\in Path(S_{\text{sour}},S_{\text{des}})\right\} \tag{5-34}$$

2）路径流量评估

路径流量评估（Link Flux Evaluation，LFE）：流X在路径P_i上各节点的带宽被认为是一致的，但流的实际频率Λ_{X_i}在各节点测得频率不等。由于信息收集模块收集信息频率F_{rc}并不和优化调整模块频率F_{ro}同步，为了使优化调整信息有效，有$F_{\text{ro}}-F_{\text{rc}}=\Delta F$。其中，$\Delta F$为两模块频率差，过大会使收集信息时效性降低，过小频繁触发优化事件会产生过优化状态，即整个系统已经接近优化状态，再次触发优化取得优化结果差别并不大。F_{ro}除了受到优化调整模块主动触发影响外，还受到流生成和交换机节点超载影响，因此F_{ro}是个动态值，为反馈函数：

$$F_{\text{ro}}=func\left(\lambda_{X_1},\lambda_{X_2},\cdots,\lambda_{X_n},F_{\text{ro}},F_{\text{rc}},TH_{s_1}^{u},TH_{s_2}^{u},\cdots,TH_{s_n}^{u}\right) \tag{5-35}$$

为了便于取值，一般使ΔF主动取值$\Delta F\in\left[0,F_{\text{rc}}/2\right]$，从而得到估计值$F_{\text{ro}}$。在可选路径$P_i$上每个节点$S_{i,j}$上测到的频率$\lambda_X(S_{i,j})$并不是相等的。其相对误差为$|\lambda_X(S_{i,a})-\lambda_X(S_{i,b})|\leqslant\Delta F$，$\forall S_{i,a},S_{i,b}\in P_i$。

流X如存在多条可选路径，则各路径必然存在至少两个以上（源和目的两个节点）重合节点。重合节点上的流X频率，接近等于该节点上所有可选路径频率之和。因此对于流X在P_i上的频率，可取非重合节点最大值：

$$\lambda_X(P_i)=\left\{\max\lambda_X(S_{i,j} \mid S_{i,j}\in P_i,S_{i,j}\notin Path(S_{\text{sour}},S_{\text{des}})-P_i\right\} \tag{5-36}$$

通过统计流在各可选路径上的概率，可估计该流在可选路径上产生的未来流量为：

$$Flux_X(P_i) = \lambda_X(P_i) b_{P_i} \tag{5-37}$$

对于路径的选择，有两种方法：

（1）最大流量

最大流量指选择该流所有经过的路径中有最大流量的路径，即选择路径：

$$P_m = \{\max Flux_X(P_i) \mid \forall P_i \in Path(S_{\text{sour}}, S_{\text{des}})\} \tag{5-38}$$

因为该流在这条路径上运行流量最大，故被认为此路径容量最适合该流，且同其他可选路径比起来，不会由于调整而被淘汰，所以最先选择该流。

（2）最佳匹配

流在运行中，流量有大有小。最佳匹配指选择流量最合适的路径，选择合适路径后，相差流量趋近为0，这样剩余流量不会被浪费。流X的流量期望为：

$$\overline{Flux_X} = \sum_{i=1}^{n} Flux_X(P_i)\lambda_X(P_i) \tag{5-39}$$

取路径：

$$P_m = \left\{\min \mid Flux_X(P_i) - \overline{Flux_X}, \mid \forall P_i \in Path(S_{\text{sour}}, S_{\text{des}})\right\} \tag{5-40}$$

以上流量取值都基于流频率参数，因此具有自适应性。

3. 流评估

传统传输方式中节点对流的处理方式是做尽力转发服务，如果节点不能承担服务则丢弃转发包，一些协议如TCP会根据丢包情况被动调节流量。这种以节点为单位的分布式控制转发方式在全局上对流进行的分析控制能力比较弱。虚拟网络能够将监控、收集信息、计算路径、转发等过程进行解耦而不损害转发性能和效率，可以专门全局性地对流进行控制，可以收集更加丰富的信息。通过这些信息集可以对流进行评价计算，独立的转发进程可根据这些评价值进行更好的流调度。同样，受到流分析粒度大小的影响，如果粒度过细，造成的系统负载和延时会过高。为了使得评价模块有效运行，这里算法只对规约到二元组的流进行评估。当一个节点在运行中超载后，控制器需要对该节点进行修正，以便该节点回到正常负载状态。

传统情况采取鸵鸟策略：最原始的方法就是交换机节点保持工作状态不变，继续对承载的流进行转发服务，该节点继续超载直到堵塞（即负载超过100%）。交换节点堵塞后会触发堵塞事件，控制器会标记该节点堵塞，再把上面承载的流调度到其他节点。此种策略下交换节点必然会出现传输堵塞事件，控制器会进行堵塞事件处理以致系统传输性能降低。

在虚拟网络中，当一个节点上的负载超过阈值时，可以对当前流进行选择，将一些

流转移到其他路径。这种方式需要对流进行评估，以便相关选择算法根据其评估值进行选择。在选择流中，算法并不复杂，一般选择权值最高、最值得排除的流。与节点评估和路径评估不同的是，流评估不仅仅注重运行时的状态，更加重视其“迁移”的困难程度。

1）流运行状态评估

控制器流评价模块评价流运行时的状态，可参考参数有流带宽、流频率、流流量和流内容等。其目的是把在当前节点状态最不好的流选出，并能使其正常工作。

（1）带宽评估

最小带宽方法（Minimum Bandwidth，Min-B）是从带宽最小的流往上选择。将当前节点流集合 $X(S)$ 占用带宽 b_{X_i} 进行排序，得到流带宽有序序列 $\{X_1, X_2, \cdots, X_N\}$。从最小到最大累加，其和第一次达到需要移动的带宽量 b_{out} 时，开始排除这些短流。设向上差值为：

$$\Delta b_{\uparrow} = \sum_{i=1}^{m} b_{X_i} - b_{\text{out}} \tag{5-41}$$

即求：

$$m = \{\min \Delta b_{\downarrow} \mid \Delta b_{\downarrow} \geqslant 0, X_i \in X(S)\} \tag{5-42}$$

通过最小带宽方法的好处是能够恰到好处地选出空间，使得空间浪费最小，因为带宽大的流移出来能够合适的路径不太多，其他节点可提供带宽都不够。缺点是这些带宽小的流需要次部署工作。最大带宽方法能够让空余的带宽可以填补更多的流，使得该节点超载的概率降低，移出流的重新部署的次数减少，缺点是被移出的带宽大的流可能没其他交换机节点有足够的剩余带宽能够承担。

（2）流量评估

通过带宽评价流运行状态不需要额外模块，但不能更加准确地评估流运行状态。当增加流量 $b_{X_i}\ \lambda_{X_i}$ 时，也可用类似带宽评估的方法进行流量评估。将带宽 b_{X_i} 参数改成流量 $b_{X_i}\ \lambda_{X_i}$ 可使用最小流量方法、最大流量方法。

2）流可管理状态评估

流管理评价主要在控制器调度流方面，当对流进行操作时会产生相应代价。一般情况下流传输是路径分配好就不再移动的，除非路径节点发生超载触发需要重新寻找路径。但当数据中心需要高效承载更多服务时，就要优化流的路径选择，这时对流的操作评价就需要考虑流移动的代价。流的“管理性质”分两种场景：一是虚拟网络系统对流可控程度，如流非正常工作管理，流转移的困难程度；二是在移动流场景中移动便捷性和移动后提高系统整体效率程度。

（1）违反服务等级协议评估

在流转发中，默认流的频率 λ_{X_i} 是基于稳定概率的，其占用带宽 b_{X_i} 也是在一定上下限范围之内的。但是，也有可能在流传输中出现奇点情况，如某一时刻带宽激增，用户本

身可能并不知道，流量不受交换机带宽限制突然增大。下面所述算法能够有效解决此类问题。

算法思想如下：设一个流Y第i次统计该流的带宽记为$b_Y(i)$，经过第n次统计，该流Y统计的平均流量为：

$$\overline{b_Y}=\frac{1}{n}\sum_{i=1}^{n}b_Y(i) \tag{5-43}$$

在第n+1次，如果流量激增，即超过本身某个限度时$b_Y(n+1)-\overline{b_Y}\geqslant\mu\overline{b_Y}+\nu$，该流被认为超过系统能够承担能力，其中参数$\mu\in R$，$\nu\in R$可以作为系统与用户的服务契约。

流X_i发生违约时，被服务等级协议模块（Service-Level Agreement Violation，SLAV）管理模块设置权值$Sl_{\text{ten}}(X_i)$，并被记录到该流的状态库中。$Sl_{\text{ten}}(X_i)$可适当取比较大的值，以便让流选择程序将该流移出繁忙节点，避免引起整个系统性能降低。

在调度流时，可通过SLAV管理模块设置权值$Sl_{\text{sys}}(X_i)$，并通过设置系统惩罚值$Penaltly(Sl_{\text{sys}}(X_i))$增加调度模块的权值来提高该流服务质量。这种方式对某一具体流具有优化性，不提高整个系统性能。

（2）流可移动性评估

流管理中有两种情况：

① 新的流X_{new}生成时，设X_{new}开始节点和目的节点分别为S_{sour}和S_{des}，因节点负载情况，系统无法通过最短路径算法创建一条最短路径P_i来负载该流。

② 对已运行的流X_t，当前所用路径为P，可选路径集合$Path(S_{\text{sour}},S_{\text{des}})$，$S_{i,j}$为路径上的某一传输节点。假设运行过程中$S_{i,j}$拥堵或者超过阈值，系统会选择另外一条可选路径$P_a$来传输流$X_t$。

传统方法中如果没有可选路径，即（1）没找到P_i或者（2）没找到P_a，系统就认为无法服务。不过在集中控制情况下，系统可尝试预判是否可以将部分权值低的流转移到其他路径，在路径P_i增加额外能力来承载流X_i服务。流的可移动性评估可通过更改流表的节点数目来参考。

第一种情况中，可选择$Path(S_{\text{sour}},S_{\text{des}})$中路径上承载流量最小的路径$P_i$尝试增加流$X_{\text{new}}$，来得到过载节点集$S_{\text{ov}}(P_i)$，从而规约到第二种情况。对每个过载节点$S_{i,j}\in S_{\text{ov}}(P_i)$上承载的所有流集合$X(S_{i,j})$中每条流$X_i$，通过路径选择算法得到新可选路径$P_a$后，有相同路径节点集合为$P_i\cap P_a$。这对于原路径$P_i$，需要在流表中减少$X_i$流表项的节点集合为$S_{\text{del}}=P_i-P_i\cap P_a$，需要在流$X_i$表中增加流表项的节点集合为$S_{\text{add}}=P_a-P_i\cap P_a$。

流转移代价定义为：

$$Mov(X_i)=Cost\left(S_{\text{add}}\right)+Cost\left(S_{\text{del}}\right) \tag{5-44}$$

在虚拟网络系统中，各节点调整流转移代价有着细微差别，与各节点流表以及整个系统的运行状态有关，本算法认为每个更改节点消耗相等。流评价权值定义为：

$$M_{Xi} = Mov(X_i) - \eta Sl_{\text{ten}}(X_i) \tag{5-45}$$

其中 $Sl_{\text{ten}}(X_i)$ 为可选值。

根据以上分析，则可以在当前节点 $S_{i,j}$ 上承载的所有流集合 $X(S_{i,j})$ 中，对所有流进行筛选和权值排序。选出权值较小的流进行移出，设有 r 个，将这些流移出后，路径空出的流量为：

$$M(X) = \sum_{i=1}^{r} b_{Xi} \lambda_{X_i}, X = (X_{\text{new}}, X_t) \tag{5-46}$$

其满足条件为：$M(X) \geqslant b_X \lambda_X$。

当移动流过多或者修改节点过多，系统可能因为修改流表消耗过多时间，修改后系统也不易恢复稳定状态。此时可通过定义移动阈值 M^{up} 来控制移动情况，当移动节点数超过 M^{up} 可判定不移动该流，即要求：

$$\sum_{i=1}^{r} \left[S_{\text{del}}(X_i) + S_{\text{add}}(X_i) \right] \leqslant M^{\text{up}} \tag{5-47}$$

当没有可选路径时，即每条流都找不到替代路径，或者找到路径但不满足 M^{up} 阈值时，则认为系统不能经过调整满足服务。

4. 调度方案

节点、流和路径等网络状态信息运算模块域管理器实现，各状态信息通过数据库储存其历史信息，其原始数据、计算数据和优化数据保存于对应的数据表中，供状态信息管理模块提取。某时刻的优化数据是通过当前网络状态数据和该时刻前一时刻优化后的历史数据计算而来的，因此不需要大量历史原始数据计算便可得到当前时刻最优值。Framework 中各模块进程独立，各模块负责结点管理、路径管理、流管理、SLAV管理功能。调度模块负责选取优化后数据进行部署。

① 信息收集模块：收集相关信息，包括节点运行状态、节点位置、链路情况、流运行状态信息等。收集信息过于频繁，会使系统全局信息比较精确，但带来的消耗也过大。在实际运行过程中，可由系统管理员设定一个初值F_0，然后根据实际运行情况及反馈信息，调整收集信息频率，避免因为收集信息带来的消耗。

② 权值计算模块：通过自适应启发式算法及收集到的信息数据库计算相关权值。

③ 优先值计算模块：将权值根据评价算法进行计算，得出最终优选结果或者优选结果集合，由调度模块选取进行部署。

其中，为了尽量缩短自适应算法样本的收集时间，需要以一定频率将各状态信息保存到数据库。模块重新启动时能够读取这些数据，这样能够获得之前已经统计的样本信息，

提高预估值精确度。估价数据库包括流经过节点、流带宽等流运行状态信息。当新流增加时可以改写新流增加事件，控制器登记同时可以直接建立流初始化信息。当一个节点没经过预估值突然堵塞时，同样可改写堵塞事件，分析堵塞原因，是哪个流引起故障，然后记录相关信息到流状态数据库，这个时候可以根据对引起堵塞的流评价 $Sl_{ten}(X_i)$ 值。

所有模块都是通过事件驱动，其中信息收集和状态计算都是线程独立模块通过一定频率触发。收集模块收集到信息后，写在原始数据库，再通过状态计算模块进行优化计算，得出一些权值和筛选后的数据集。调度模块再根据事件处理函数选择这些数据集进行合理计算，得出结果后重新部署。在实现算法评价时，关注的事件如下：

① 节点堵塞。节点堵塞由系统本身触发事件，可改写节点堵塞事件处理函数，标记引发堵塞的流，并通过流评价模块得到流权值，根据这些权值选择一个或者多个流进行分流。

② 节点超载。即节点超过阈值，与节点堵塞不同的是节点超载时节点还可以继续工作。该事件由监控模块发起预警事件，并由调度模块处理，处理方式同节点堵塞事件。

③ 新建流。当节点有新建流时，系统触发新建流事件。可改写该事件：最短路径算法读取的权值改为状态计算模块算出的值，当最短路径算法找不到路径时添加分流算法。

5.9.4 终端通信接入网路由优化策略研究

终端通信接入网所承载的业务具有高可靠性和低时延的需求，为保证业务的QoS以及网络的整体性能，本部分以终端通信接入网业务传输时间的紧迫程度为主，辅以业务通信量、安全性要求及数据失效对电网的影响，将业务划分为以时延为表征区分的四类，同时以业务风险均衡度和业务平均风险度为终端通信接入网的可靠性评估指标，提出了一个终端通信接入网路由优化算法。该算法在时延需求的约束下，综合考虑业务的QoS要求以及网络的整体性能，将网络时延、平均风险、业务风险均衡度作为路由优化的目标函数，建立终端通信接入网路由优化模型，然后利用多目标遗传算法求解出一组最优的路由组合方案，实现业务路由优化分配。最后，基于上述处理，提出适用于终端通信接入网的路由优化策略，从业务层面为业务可靠性评估和网络运行方式优化提供理论参考。

1. 路由优化模型及其算法实现

1）路由优化模型

在终端通信接入网中，单点传输的通信量普遍较小，但节点覆盖范围广，终端数目众多，总信息量大，行为复杂。以终端通信接入网业务传输时间的紧迫程度为主，辅以业务通信量、安全性要求及数据失效对电网的影响（即业务的重要性），将其划分为四类，紧急类、重点类、标准类和适度类，分别用type=1，2，3，4表示，同时将时延作为表征区分各类业务的重要指标。

随着终端接入网的发展，电力业务的种类和数量迅速增加，传统通信网中将“路径最

短”作为路由策略，缺乏对网络整体性能的考虑。在区分业务模型下，业务的价值有所不同，因此不能直接根据传统的优化目标制定衡量指标，应当结合业务价值进行衡量指标的计算。此处在进行电力业务的路由选择时，除了考虑每一个业务的QoS要求（主要是时延性能）外，还兼顾整个网络的平均风险和风险均衡度，建立了更加全面完整的优化模型。

对终端通信接入网进行路由优化的目的在于调节业务QoS和网络整体性能之间的关系，找出一组能够使多个目标函数同时取得较优结果的解集。

（1）网络时延

通信技术快速发展使得终端通信接入网建设、维护水平也相应提高，电力业务在带宽、可靠性要求等方面的紧张状况得以缓解，而时延则成为影响电力业务QoS的关键因素。

终端通信接入网业务对时延有明确的要求。配网保护业务要求传输时延在40ms以内，调度电话要求传输时延在500ms以内，这就对电力业务路由的距离和跳数做出了约束，在为业务选择路由时必须满足业务的时延性能。根据业务对于时延的不同要求，可以容易地实现对业务的分类。

将网络中的业务按照时延等级要求分为M类，第$i(1 \leqslant i \leqslant M)$类业务的总量为$N_i$，研究中用跳数表征时延。给第$i$类的第$j$个业务分配一条路由，$h_{ij}$为业务采用该路由时的跳数，则第$i$类业务的平均跳数为：

$$D_i = \frac{1}{N_i}\sum_{j=1}^{N_i} h_{ij} \tag{5-48}$$

给网络中的所有业务分配路由以后，定义网络时延为：

$$D = \sum_{i=1}^{M} wt_i D_i \tag{5-49}$$

其中，wt_i是第i类业务的业务价值。

$$wt_i = \frac{1}{H_i} \tag{5-50}$$

其中，H_i为第i类业务时延上限对应的跳数最大值。

（2）网络平均风险

通信网中的风险是指由网络的脆弱性、人为或自然的威胁导致故障发生的可能性及其影响。为缩小计算规模，假设终端通信网中的故障主要是指链路故障。链路故障影响的评估以链路上业务重要度的划分为基础。在终端接入网中，承载的业务种类相对比较简单，且具有明显的特征，这使得对电力业务的重要度评价成为可能。

在传统的链路风险评价中，对于链路l，经过链路的第i类业务数量为N_i^l，其业务价值为wt_i，链路失效概率为f_l，利用相乘法原理定义链路风险：

$$r_l = f_l \sum_{i=1}^{M} \left(N_i^l wt_i \right) \tag{5-51}$$

这种定义方式只注重链路本身的可靠性与风险之间的关系，却忽略了链路的拓扑属性对风险的影响。在实际的网络运行中，当链路发生故障以后，可以通过保护、恢复的方式重建业务路由，降低故障损失。然而网络中链路的容量是有限制的，故障发生后很难做到100%恢复。链路的介数表示网络中节点间的最短路径经过该链路的次数。链路介数越高，可能承载的业务越多，该链路中断以后，由于链路资源限制导致重路由失败的可能性也越大。此外，还要考虑到网络受到攻击的可能性。攻击者在掌握网络拓扑但不知道具体业务分布的情况下，往往会优先攻击介数高的链路，导致这些链路的风险要高于介数较低的链路。利用介数对链路风险的定义进行修正，更能反映网络运行的实际情况。研究旨在调整业务的路由分配，关注的是链路风险的相对值，同时为了避免数值过大，所以采用归一化处理后的边介数对式（5-51）进行修正，将其作为反映网络脆弱性的一个指标。链路风险重新定义为：

$$r_l = \overline{b_l} f_l \sum_{i=1}^{M} \left(N_i^l w t_i \right) \tag{5-52}$$

其中 $\overline{b_l}$ 为归一化的边介数：

$$\overline{b_l} = \frac{b_l}{\max\{b_k\}} \qquad k = 1, 2, \cdots, L \tag{5-53}$$

则对于有L条链路的网络，平均风险可以定义为：

$$R = \frac{1}{L} \sum_{l=1}^{L} r_l \tag{5-54}$$

（3）业务风险均衡度

为了保证业务的时延性能，业务通常是选择最短路径的静态路由。这样虽然保证了业务的时延性能，但是会导致业务过度集中在少数几条链路上。这些链路就成为接入网的薄弱环节。此外，由平均风险的定义可知，业务选路时，优先选择介数低的链路有助于降低网络的平均风险，当介数低的链路上集中了大量业务时，平均风险值大幅降低。但是当这些链路发生故障以后，同样会造成大量业务损失，导致网络性能急剧下降。可见一味地追求降低平均风险并不能改善网络的脆弱性，所以，定义风险均衡度应作为表征网络脆弱性的另一个重要指标。对于有L条链路的网络，在计算出链路平均风险的基础上，用链路风险均方差的无偏估计来表示风险均衡度：

$$BR = \sqrt{\frac{1}{L-1} \sum_{l} (R - r_l)^2} \tag{5-55}$$

风险均衡度反映了网络的风险值在链路之间均匀分配的程度。

利用全网业务风险度均衡度可以从网络业务的风险度及风险分布均衡度两个方面对网络总业务分配均衡性进行度量。业务风险均衡度指标能够反映网络中各业务通道段所承载的业务风险度均衡分布情况，如果该指标值过高，则表示网络中业务通道上承载的业务分

布不均，个别链路上重载，或个别链路上轻载，或个别链路上重要业务（高业务重要度）过于集中；如果该指标值趋于 0，则表示全网的业务安排风险均衡，网络运行风险较小。

业务对时延的要求严格而明确，在给业务分配路由时必须满足该业务的时延要求。在此约束条件下，综合考虑业务的QoS要求以及网络的整体性能，本书将网络时延、平均风险、业务风险均衡度作为路由优化的目标函数，则终端通信接入网路由优化问题可以建模如下：

$$\begin{cases} \min D = \sum_{i=1}^{M} wt_i D_i \\ \min R = \dfrac{1}{L}\sum_{l} r_l \\ \min BR = \sqrt{\dfrac{1}{L-1}\sum_{l}(R-r_l)^2} \\ \quad s.t. \quad h_{ij} \leqslant H_i \end{cases} \tag{5-56}$$

2）算法实现

进行路由优化的目的在于调节业务QoS和网络整体性能之间的关系，找出一组能够使多个目标函数同时取得较优结果的解集。混沌遗传利用混沌序列的随机性、遍历性，能够改善传统遗传算法中的局部收敛问题，达到很好的寻优效率。研究将混沌遗传算法应用于路由优化问题中，得到一组pareto最优解，以便进行最终决策。在优化算法中，把需要进行路由调整的业务作为决策变量，决策变量的不同取值对应该业务的不同路由方式。协同进化过程中，子种群的数量即为决策变量的个数，子种群中的不同个体对应该决策变量的不同取值。子种群合作形成的完整解代表所有待调整业务的一种路由组合。通过多目标算法，求解出一组最优的路由组合方案。

（1）染色体编码与解码

对于业务 i，若备选路由数量为N_{iR}，则决策变量的取值范围是$\left[0, N_{iR}-1\right]$区间上的所有整数。以图5-21中节点对A-E之间的某个业务s为例，假设其所有满足时延要求的备选路由方案为A-B-E，A-G-F-E，A-C-D-E，则业务s对应的基因上的变量取值范围为整数{0, 1, 2}。

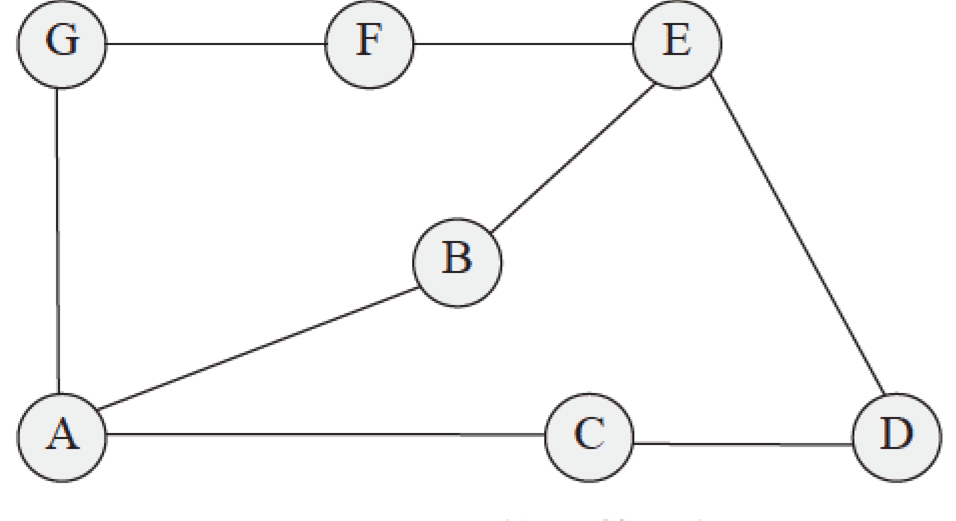


图5-21　网络拓扑实例

由于在协同进化中，每个决策变量对应一个子种群，所以子种群中每个个体染色体基因的数量为1。针对变量取值为整数的实际情况，以及为了处理方便，采用二进制编码，

一条染色体的长度为：

$$L = N_c \tag{5-57}$$

其中，N_c 为基因的编码长度，其取值要求为：

$$2^{N_c - 1} < \max_i N_{iR} \leqslant 2^{N_c} \tag{5-58}$$

在进行染色体的解码时，将子种群i中第j个个体的二进制基因解码为十进制数x_{ij}_dec。对于业务m，如果其可用路由数$N_{mR} < \max_i N_{iR}$，会出现子种群m中第n个体基因的解码值$x_{mn}_dec > N_{mR} - 1$的情况，为了避免变量越界，保证变量在$\left[0, N_{mR} - 1\right]$的范围内，将其解码为$\mathrm{mod}\left(x_{mn}_dec, N_{mR}\right)$，即$x_{mn}_dec$对$N_{mR}$求取余数。所以，子种群$i$中个体的染色体解码方式为：

$$x_{ij} = \begin{cases} x_{ij}_dec & x_{ij}_dec \leqslant N_{iR} - 1 \\ \mathrm{mod}\left(x_{ij}_dec, N_{jR}\right) & x_{ij}_dec > N_{iR} - 1 \end{cases} \tag{5-59}$$

（2）种群的初始化与合作方式

利用混沌序列完成种群的初始化，所选混沌方程为：

$$\begin{cases} x = -ax + by + yz \\ y = cx - dy - xz \\ z = ex - fz - g\,xy \end{cases} \tag{5-60}$$

式中，$a = 10, b = 16, c = 40, d = 4, e = 5, f = 5, g = 7$。

当系统进入混沌状态以后，对变量x进行采样得到混沌序列。对于子种群i，设其容量为M，则需要编码的位数为MNc，对混沌序列进行长度为MNc的采样，获取混沌变量矩阵：

$$\begin{pmatrix} x_{11}^i & x_{12}^i & \cdots & x_{1N_c}^i \\ x_{21}^i & x_{22}^i & \cdots & x_{2N_c}^i \\ \vdots & \vdots & \ddots & \vdots \\ x_{M1}^i & x_{M2}^i & \cdots & x_{MN_c}^i \end{pmatrix}$$

利用式（5-61）将混沌变量映射到$(0,1)$范围内。

$$x' = \frac{x - a}{b - a} \qquad x \in (a, b) \tag{5-61}$$

初始子种群P^i按式（5-62）完成种群的初始化：

$$p_{uv}^i = \begin{cases} 1 & x_{uv}^{i\,\prime} \geqslant 0.5 \\ 0 & x_{uv}^{i\,\prime} < 0.5 \end{cases} \quad \left(u = 1, 2, \cdots, M, v = 1, 2, \cdots, N_c\right) \tag{5-62}$$

子种群间合作方式如图5-22所示。对于有n个决策变量的多目标优化问题，生成n个容量为M的子种群，通过将子种群中的个体随机组合，生成容量为M的完整解种群。设置外部存储器，容量为M。从随机组成的完整解种群中，选择非支配解，存入外部存储器，完成外部存储器的初始化。

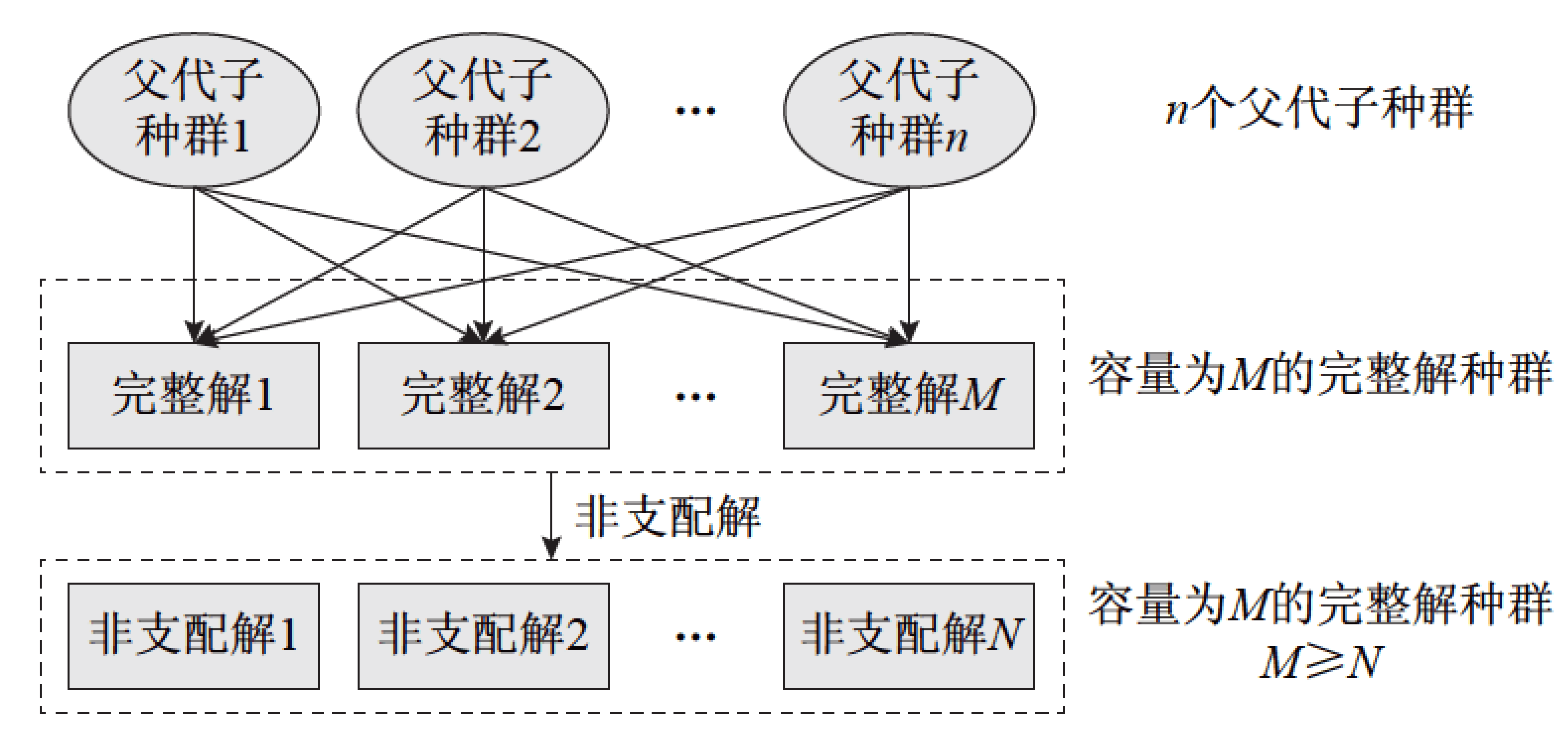


图5-22　子种群合作方式

（3）种群的交叉变异（自种群和外部存储的更新）

初代子种群和外部存储器的初始化完成以后，算法进入繁殖进化阶段。如图5-23所示，父代子种群经过变异、交叉，生成子代子种群。从子代子种群中随机挑选相应的决策变量，组合形成新一代的完整解种群。

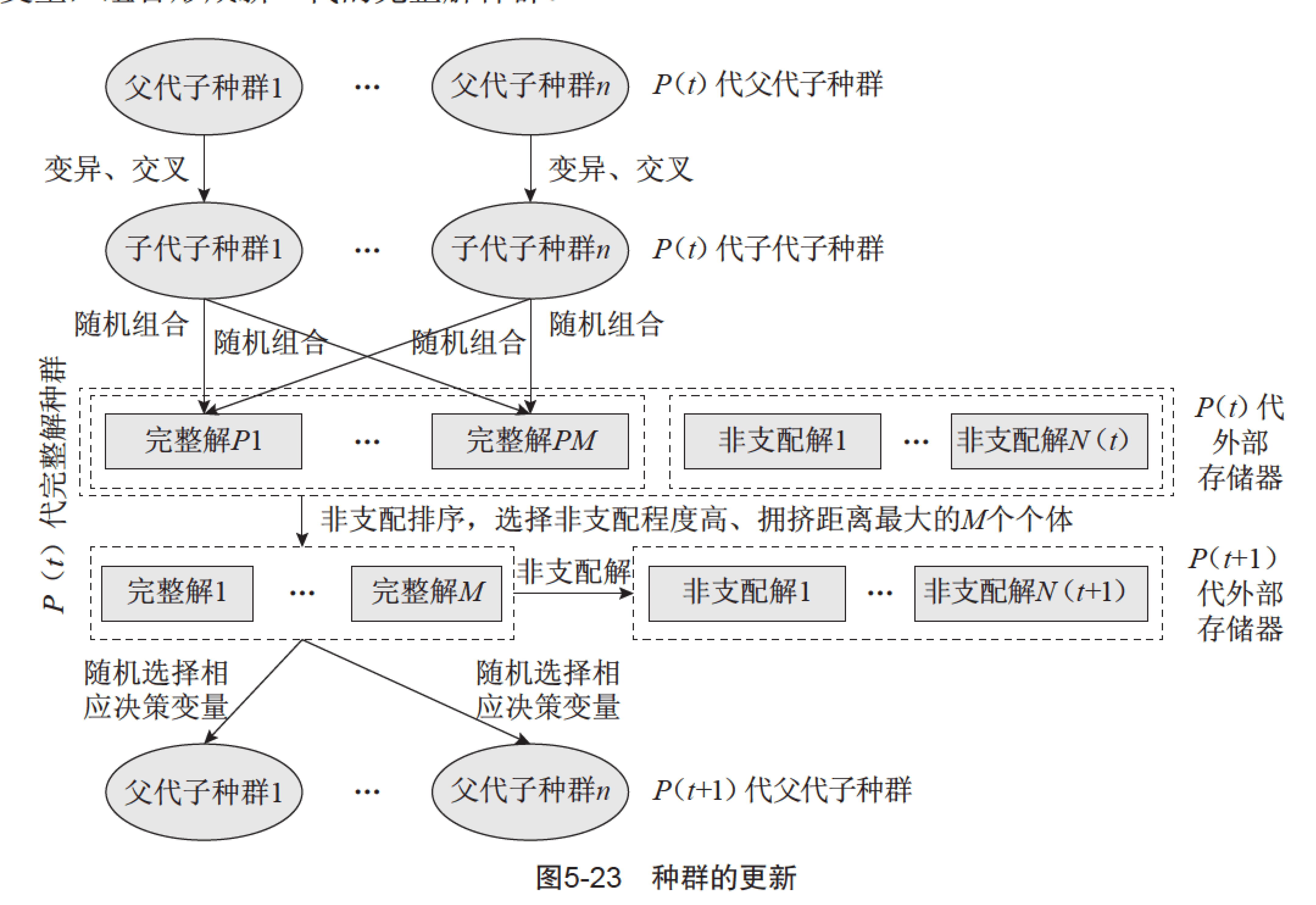


图5-23　种群的更新

为了充分利用外部存储器中保留的精英个体，将外部存储器中的个体与当前的完整解种群混合，进行选择操作。借鉴NSGA-Ⅱ中非支配排序的思想，对混合种群进行聚类分

层，计算每层内部的拥挤距离并排序。非劣层次越低，拥挤距离越大的个体，其非支配程度越强。对于边界个体，为了保证种群的多样化，将边界个体的拥挤距离设为无穷大以确保其能够以较大的可能性遗传到下一代中。这保证了进化算法能够在当前较优解的基础上进一步发掘出更加优秀的个体。将混合种群中的非支配个体存入外部存储器，实现对外部存储的更新。在进化过程的早期阶段，外部存储器中的非支配个体较少。但是随着迭代次数的增加，非支配个体的数量会逐渐超过外部存储器容量M的限制，此时只需要选择其中拥挤距离最大的M个个体进行存储，然后根据非支配排序的结果，从混合种群中选择非支配程度最强的M个个体，将它们的决策变量分配到相应的子种群中，形成新的父代子种群。

（4）支配解的混沌变异

得到新的父代子种群后，为了扩大寻优能力，对下一代的父代子种群中，来自支配解和非支配解的决策变量采取不同的变异策略。对于来自非支配解的决策变量进行自适应概率的变异操作，变异概率为：

$$p_m = p\exp(-t/T) \tag{5-63}$$

其中p的取值为决策变量个数的倒数，$\exp(-t/T)$是尺度调节算子，t是当前的遗传代数，T是总的遗传代数。

对来自支配解的决策变量进行混沌变异，利用混沌序列的遍历性避免传统遗传算法中出现的局部收敛。对于子种群中来自支配解的决策变量$P_i=\{p_{i1},p_{i2},\cdots,p_{iN_c}\}$，先从混沌序列中抽样，并映射到（0，1）范围内，产生混沌变量$Y_i=\{y_{i1},y_{i2},\cdots,y_{iN_c}\}$，按式（5-64）对$P_i$进行变异：

$$p_{ij}=\begin{cases}1-p_{ij} & y_{ij}<p\exp(-t/T)\\ p_{ij} & y_{ij}>p\exp(-t/T)\end{cases} \tag{5-64}$$
$$j=1,2,\cdots,N_c$$

尺度调节算子的引入，目的是在算法的初期尽可能地扩大搜索范围，避免陷入局部最优，在算法的末期提高局部微调的能力，加快算法收敛。

2. 终端通信接入网路由优化策略

1）路由优化策略流程

终端通信接入网承载着大量的实时生产控制业务，对于电网的安全稳定运行起着至关重要的作用，对于这些业务，调整其路由时需要慎之又慎。在优化过程中，调整的业务路由过多时会使算法复杂度上升，降低优化算法效率。为了降低路由调整对电网正常运行的影响，同时也降低决策变量的个数，提高搜索效率，应当选择风险值较高的链路上的业务进行调整。

基于上述染色体编解码、种群合作方式、种群更新以及混沌变异等处理，终端通信接入网的路由优化策略流程如下：

① 针对拓扑、业务已知的终端通信网，计算链路的风险值，选择链路风险值较高的k条链路，记录经过这些链路的业务，生成待调整业务向量集$\{s_1,s_2,s_3,\cdots,s_n\}$，$n$为待调整的业务数量。为$\{s_1,s_2,s_3,\cdots,s_n\}$中的业务计算所有满足时延要求的可用路由并存储编号，将路由方案编号作为优化算法中决策变量的取值。

② 种群的初始化。令进化代数t=1，对应于n个业务，随机产生n个个体数量为M的初始父代子种群。设立外部存储器A，其容量为M。初始父代子种群中的个体随机组合，形成M个完整解，计算每个完整解的目标函数向量，选择其中的非支配解，存入外部存储器A中。设置最大进化代数T。

③ 种群的繁殖操作。子种群合作产生M个完整解，与外部存储器中的精英个体混合，计算目标向量，进行非支配排序，选择非支配解完成外部存储的更新。保留非支配程度最强的M个个体，将决策变量分配到相应的子种群中，形成下一代的父代子种群。对于来自非支配解的决策变量，进行自适应概率变异；来自支配解的决策变量，进行混沌变异。对变异以后的父代子种群进行均匀交叉，生成n个子代子种群。

④ 终止判断。如果t=T，则把当前外部存储器A中的个体作为pareto最优解集输出，否则转到③，进化代数$t=t+1$。

⑤ 进行决策，从输出的N个最优解中，选择方案k为最终的优化方案。

$$k=\arg\min\left\{\frac{f_1(x_i)}{f_{1\min}}+\frac{f_2(x_i)}{f_{2\min}}+\frac{f_3(x_i)}{f_{3\min}}\right\}\qquad i=1,2,\cdots,N \tag{5-65}$$

其中x_i是pareto最优解集中的个体。

2）算例分析

以图5-24所示的拓扑为例，网络中节点个数为7，业务通道边的数目为10。设网络中有4个业务需求，分别为：节点N1到N6的紧急业务；节点N1到N5的重点业务；节点N1到N4的标准业务；节点N1到N7的适度业务。利用遗传算法并根据上述路由优化策略流程进行路由优化分配，表5-29给出了各pareto最优解对应的路由优化方案。

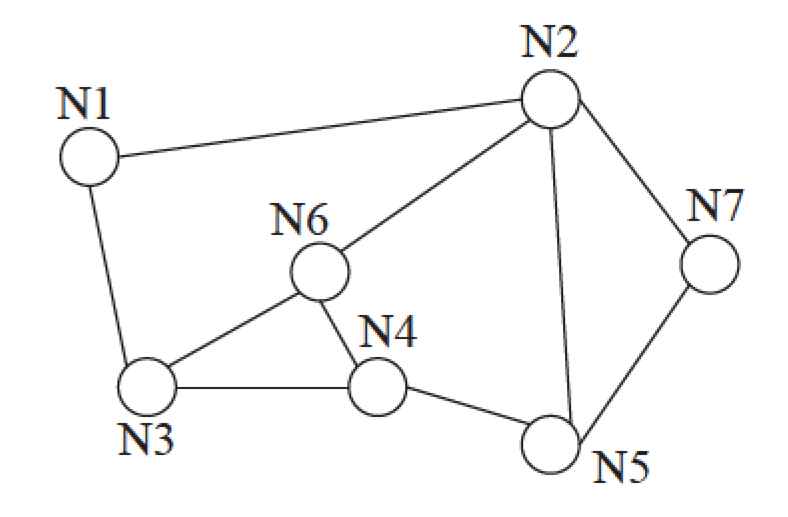


图5-24 终端通信接入网拓扑图例

表5-29　各pareto最优解对应的路由优化方案

业务	方案1	方案2	方案3	方案4	方案5
紧急业务	N1—N2—N6	N1—N3—N6	N1—N3—N6	N1—N2—N6	N1—N3—N6
重点业务	N1—N2—N5	N1—N3—N4—N5	N1—N2—N5	N1—N3—N4—N5	N1—N3—N4—N5
标准业务	N1—N3—N6—N4	N1—N2—N6—N4	N1—N2—N5—N4	N1—N3—N4	N1—N2—N6—N4
适度业务	N1—N3—N4—N5—N7	N1—N3—N6—N2—N7	N1—N3—N6—N4—N5—N7	N1—N3—N4—N5—N2—N7	N1—N2—N5—N7

5.10 总　　结

本章针对电力终端通信接入网规划进行了详细讨论，总体分为三部分：①业务对接入网的性能需求；②接入网业务保障机制；③网络规划原则。

在第一部分（5.1节～5.5节）对终端通信接入网业务需求特征分析方面，通过相关调研，研究了各类业务在传输速率、系统容量、通信时延和安全稳定等通信传输特征需求上的差异性。根据不同的业务特征需求，提出了现有电力生产运行业务、企业管理信息类业务的新型需求和未来能源互联网下的新型业务及其特征需求，并提出了相应的业务质量评价指标，包括业务QoS评价、业务重要度等。

在第二部分（5.6节和5.7节）研究了基于业务等级的分组调度策略、基于业务等级的BS-WFQ调度策略以及队列管理方法。

在第三部分（5.8节和5.9节）提出了面向终端通信接入网多业务接入的路由选择优化策略。该策略考虑到当前时刻的网络节点及链路的实际负载情况和网络负载的动态变化情况以及网络中各类网络路由节点存储转发能力的差异性，通过优化网络数据转发经过节点数和转发路径来实现业务低时延通信要求，并考虑了链路风险性评估来保证业务高可靠性传输。为实现资源的统一管理与调度，这里提出了基于虚拟化的综合网络优化策略。利用虚拟化技术建立面向终端通信接入网的网络虚拟化的分层模型，将底层物理网络进行逻辑抽象，从而在共享的基础设施上创建和运行多个不同的虚拟网络；并在此基础上提出了基于资源分配的虚拟网络映射算法与面向流的虚拟网络调度方案，将虚拟网络请求映射到基础设施上，利用已有的物理资源获得更多的业务收益，实现了网络统一管理与资源共用。

第6章
典型组网模式



6.1 终端通信接入网典型场景

6.1.1 配电自动化应用场景

配电自动化是指以一次网架和设备为基础，综合利用计算机、信息及通信等技术，并通过与相关应用系统的信息集成，实现对配电网的监测、控制和快速故障隔离。配电自动化系统主要由配电自动化系统主站、配电自动化终端和配套通信网络等组成。

配电自动化的典型应用场景包括：

① 在A+类供电区域，以EPON、工业以太网交换机等光纤通信技术为主进行组网。

② 在A、B、C类供电区域，三遥终端优先采用光纤通信方式，载波和无线通信作为补充，采用载波方式进行补充时不宜进行规模组网。二遥终端可采用光纤和无线融合方式、光纤和载波融合方式。

③ 在D、E类供电区域，以无线或载波通信方式为主。

对于需要实现三遥功能的配电自动化站点，网络安全性、可靠性的要求很高，优先采用光纤通信方式（EPON或工业以太网交换机）。对于不需要遥控功能的二遥站点，可采用光纤+无线方式，中压电力线载波作为辅助接入方式。

6.1.2 用电信息采集应用场景

用电信息采集覆盖所有电力用户、电网各类计量点以及包括电动汽车充电设施、分布式电源及微电网等。用电信息采集系统从物理上可根据部署位置分为主站、通信信道、采集终端三部分。

典型应用场景应覆盖六大类用户：大型专变用户、中小型专变用户、三相一般工商业用户、单相一般工商业用户、居民用户、公用配变考核计量点。

① 大型专变用户：需实现对计量电表的远程抄表，实时用电电量、负荷数据的采集，计量工况等现场事件信息的采集，用户用电负荷控制和用电量控制，提供本地信息服务等功能。终端与主站之间可采用专用光纤网络、230MHz无线专网等通信方式。

② 中小型专变用户：需实现对计量电表的远程抄表、强化计量工况和现场事件的信息采集、支持预付费功能、具有必要的本地信息服务等。终端与主站之间可采用专用光纤网络、布设无线专网等通信方式。

③ 三相或单相一般工商业用户：需实现对计量电表的远程抄表，强化对用电信息、计量信息的实时采集和异常分析。在系统主站的监控下，通过电表的直接控制实现完整的预付费管理功能。终端与主站之间可采用专用光纤网络、假设无线专网等通信方式。

④ 居民用户和公用配变考核计量点：需实现居民计量电表的远程抄表和预付费控制管理功能，实现对配变台区考核总表的远程抄表和用电信息采集。终端与主站的远程通信可采用专用光纤网络等。

6.1.3 电动汽车充电站应用场景

电动汽车充电站分为集中充电站和充换电站，充电站按照“以自建电力光纤专网方式为主，租用公网运营商通信网络方式为辅”的模式，运营管理系统部署于地市公司。

电动汽车充电站典型应用场景：

① 集中充电站主要位于110/220kV变电站附近，从变电站引入双路10kV电源进行供电，该类站点作为电池集中充电和供应站点，数量较少，对安全性和实时性要求高，因此采用自建SDH光纤专网方式就近接入变电站电力骨干通信传输网络。

② 充换电站由上级电源点（35/110/220kV变电站、10kV开闭所等）引双路10kV电源或1路10kV加1路0.4kV电源进行供电，对安全性和实时性要求较高，采用自建SDH光纤专网方式就近接入变电站电力骨干通信传输网络。

③ 对于上级电源点为10kV开闭所且该开闭所不具备至变电站光缆通道的主城区充换电站，以及城际高速公路充换电站，采用租用运营商专线通道，通过安全隔离设备接入运营管理中心，充电站部署通信交换机接入到运营商的网络。

6.1.4 电动汽车充电桩应用场景

电动汽车充电桩是电动汽车服务网络的末端充电设施，数量多且位置分散，分布在社区停车场、公共设施停车场等处，采用单路0.4kV电源引入方式，对安全性要求较高，实时性要求一般。

电动汽车充电桩主要采用自建的EPON设备和租用的运营商网络进行信息的采集和传输，接入到运营管理中心。

电动汽车充电桩典型应用场景：

① 充分结合终端通信网资源自建电力光纤专网，不具备终端通信网资源则考虑布设无线专网模式。

② 当充电桩所在区域具备终端通信接入网络资源时，充电桩上级电源点为10kV开闭所，且该开闭所具备至变电站光缆通道时，采用自建EPON光纤专网方式就近接入变电站电力通信传输网络。

6.1.5 分布式电源接入应用场景

分布式发电站接入通信设备、线路等不考虑双重化配置，通道一般按单路配置。分布式发电站侧的通信设备型号应与电网侧保持一致性，配套的电源、配线设备以及相关的运行环境等按能够保障通信设备连续、安全稳定运行的要求配置。

分布式电源典型应用场景：

① 在分布式电源密集部署且光缆易于敷设的区域，或在配电自动化光纤网络已覆盖的区域，优先选择EPON或工业以太网技术。

② 在分布式电源相对分散且具备光纤网络，但不宜采用EPON技术的区域，优先选择SDH传输技术。

③ 在分布式电源相对分散且光缆线路难以敷设的区域，可选用中压电力线载波方式。

④ 在分布式电源密集且光缆敷设困难的区域，可选择无线专网。

⑤ 对10kV电压接入的分布式电源，若无控制业务需求，可考虑布设无线专网；对380/220V低压接入分布式电源，可以选择布设无线专网。

6.1.6 配用电多业务接入应用场景

公共接入平台利用现有通信技术，统筹考虑配电自动化、用电信息采集、电动汽车充电站（桩）、分布式电源接入等不同业务应用需求，研究通信资源优化配置策略、业务隔离、数据加密、通道安全防护等关键技术，实现不同业务的集中接入和资源共享。

终端通信接入网公共接入平台重点研究基于EPON、工业以太网、无线专网技术的配用电业务共网承载方案，以及对应的安全防护技术。

终端与信息内网业务系统间的每一个数据交互过程都是业务数据安全接入的过程。终端通过接入公共接入平台，根据平台的认证、通信数据加密等安全方式，实现与内网业务系统的安全数据交互。

汇总终端通信接入网各类典型场景适用的接入技术如表6-1所示。

表6-1 终端通信接入网各类典型场景及适用技术

业务类型	场景	是否有光纤资源	接入技术
配电自动化	A+类供电区域	有	EPON或工业以太网
	A、B、C类区域三遥功能	有	EPON或工业以太网
		无	载波或无线
	A、B、C类区域二遥功能		光纤+无线/载波
	D、E类区域	无	无线或载波

续表

业务类型	场　　景	是否有光纤资源	接入技术
用电信息采集	大型专变用户	有	EPON或工业以太网
		无	无线专网
	中小型专变用户	有	EPON或工业以太网
		无	无线专网
	三相和单相一般工商业用户	有	EPON或工业以太网
		无	无线专网
	居民用户和公用配变考核计量点	有	EPON或工业以太网
		无	无线专网
电动汽车充电站	集中充电站、充换电站	有	SDH光纤专网
	主城区充换电站、城际高速公路充换电站	无	无线专网
电动汽车充电桩		有	EPON
		无	无线专网
分布式电源接入	分布式电源密集	有	EPON或工业以太网
	分布式电源密集	无	无线专网
	分布式电源相对分散	有	SDH
	分布式电源相对分散	无	中压电力线载波
	10kV电压接入的分布式电源，无控制业务需求	无	无线专网
	380/220V低压接入分布式电源	无	无线专网

6.2　终端通信接入网技术特征分析

6.2.1　EPON技术特征

EPON采用点到多点结构，无源光纤传输方式，在以太网之上提供多种业务。EPON技术融合了低成本、高带宽的以太网设备和低成本的光纤网技术，是接入网技术的一种，相对于其他接入技术具有独特的优势，主要体现在组网可靠性、带宽分配、通信实时性，动态带宽分配技术、测距技术、QoS技术、加解密技术、承载TDM业务技术、光纤保护倒换技术方面；相对成本低，维护简单，容易扩展，易于升级；只需更改光分路器就能增加光方向，从而增加终端节点。但是EPON工程建设周期相对较长，一次性投入相对较大，光缆线路维护困难。

EPON系统由网络侧的光线路终端（OLT）、用户侧的光网络单元（ONU）和光分配网络（ODN）组成。下行方向（OLT到ONU）采用广播的方式，OLT发送的信号通过ODN

到达各个ONU。在上行方向（ONU到OLT）采用TDMA多址接入方式，ONU发送的信号只会到达OLT，而不会到达其他ONU。

如图6-1所示，ODN为OLT侧的S/R点至ONU侧的R/S点之间的网络，主要由光缆、光缆接头盒、光分路器、光缆线路终端分配设备、光缆交接箱、光缆分纤箱、光分路箱（框）等组成。

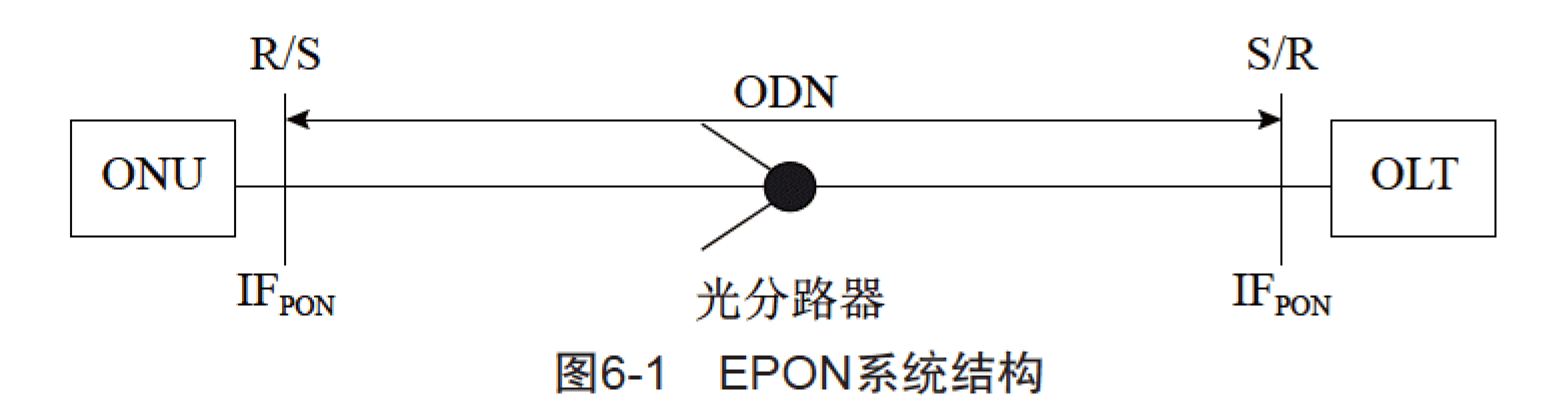


图6-1 EPON系统结构

在选择ODN结构时，应根据用户性质、用户密度的分布情况、地理环境、管道资源、原有光缆的容量，以及OLT与ONU之间的距离、网络安全可靠性、经济性、操作管理和可维护性等多种因素综合考虑。

EPON网络可以灵活组成树型、星型、总线型等拓扑结构。

6.2.2 工业以太网技术特征

工业以太网是应用于工业控制领域的以太网技术，在技术上遵循IEEE 802.3标准，可以在光缆和双绞线上传输，针对工业环境对工业控制网络可靠性能的超高要求，加强了冗余功能。工业以太网在技术上与以太网兼容，在网络规划设计、材质选用等方面需要充分兼顾实时性、互操作性、可靠性、抗干扰等工程应用的需要。工业以太网交换机具有技术成熟、性能稳定、组网灵活、便于升级扩容等优点，具有耐高温、潮湿环境、强电磁干扰等恶劣环境的特点，使用的是透明而统一的TCP/IP协议。

工业应用对数据传输的实时性、可靠性提出了很高的要求，以太网作为一项成熟的网络方案，其诸多技术可以满足工业应用的需求，还具有网络性能好、相关设备元件成本低、不同设备之间互连互通性好等特点，因此成为工业控制领域数据传输方案的出色选择之一。相较于以RS-232或RS-485为基础的工业网络，工业以太网络有以下的优点：

① 提升传输速率。RS-232的速率为9.6kbps，若是吉比特以太网，使用CAT-5e、CAT-6的网络线或光纤为传输介质，传输速率可以到1Gbps。

② 传输距离可以拉长。可以使用标准的路由器、以太网交换机、集线器、网线及光纤。除了传统的主－从结构（master-slave）外，也可以使用点对点技术。

③ 较好的互操控性。

但需要指出，应用工业以太网时也有一些缺点：

① 如果已有协议非以太网协议，则系统移植成本高。

② 在及时控制领域使用像TCP协议时复杂度高（有些应用因此使用UDP或其他数据链

路层的协定），处理TCP/IP数据包会比处理串行数据要复杂很多。

③ 最小的以太网帧大小为64个字节，但一般工业控制数据只有1～8个字节，协议开销（protocol overhead）会影响数据传输的速率。

6.2.3　无线专网技术特征

电力无线专网包括LTE、Mcwill、Wimax等技术，考虑到标准化程度、技术成熟度、产业链等因素，从技术长远发展的角度来考虑，主要采用基于TD-LTE核心技术的电力无线专网LTE，主要包括230MHz、1.8GHz频段，要求支持技术的平滑演进。

无线专网的网络架构可采用下一代无线通信的C-RAN架构，使网络结构扁平化，能够降低时延，网络覆盖力更强，减少网络投资成本。电力宽带无线通信系统主要由无线终端UE、无线基站eNodeB（包括BBU和RRU）、核心网EPC及网管eOMC构成。

从频谱特性、覆盖能力、峰值传输速率、端到端时延、用户容量、投资成本、扩容能力、产业链几个方面概括230MHz、1.8GHz频段专网LTE的技术特点如下：

（1）频谱特性

230MHz频段LTE：占用223～235MHz范围的电力专用频谱，电力能源行业拥有其中40个授权频点，25kHz为1个频点范围，共1MHz带宽。

1.8GHz频段LTE：占用1785～1805MHz范围的公用频谱，有20MHz连续频率（TD-LTE系统规范支持定义了6种系统带宽，包括1.4MHz、3MHz、5MHz、10MHz、15MHz、20MHz，TD-LTE网络可灵活选择带宽）。

（2）覆盖能力

230MHz频段LTE：230MHz频段范围的基站覆盖能力更强，密集城区覆盖半径约3km，郊区约10km，农村约30km。

1.8GHz频段LTE：1.8GHz频段范围的基站覆盖能力相对较弱，密集城区覆盖半径约1km，郊区约4km，农村约6.6km。

（3）峰值传输速率

230MHz频段LTE：上行峰值速率14.96Mbps，下行峰值速率5.8Mbps（8.5MHz带宽时）。

1.8GHz频段LTE：上行峰值速率8.5Mbps，下行峰值速率12.5Mbps；或上行峰值速率7.1Mbps，下行峰值速率20Mbps（带宽5MHz时）。

230MHz系统上行速率大于下行速率的特点，较符合配电自动化网中的业务速率特点。

（4）端到端时延

TD-LTE系统时延在ms量级。

（5）用户容量

用户实时在线，每个逻辑小区能支持1000个以上的用户。

（6）投资成本

230MHz频段LTE：由于覆盖能力更强，站点少，可以充分利用电力的现有基础设施，综合来说投资成本较低。

1.8GHz频段LTE：由于覆盖能力较弱，站点多，需要新建机房、铁塔等基础设施，综合来说投资成本较高。

（7）扩容能力

230MHz频段LTE：扩容需要新建较少的基站。

1.8GHz频段LTE：扩容需要新建较多的基站。

（8）产业链

230MHz频段LTE：产业链尚未形成，制造厂商较少。

1.8GHz频段LTE：国外、海外应用广泛，产业链成熟，目前已有华为、中兴、大唐、鼎桥、普天等厂商可以提供端到端成熟的产品。

6.2.4 技术特征总结

在电力终端通信接入网应用中，EPON和工业以太网具有技术成熟、安全性和实时性高、传输距离较远、成本相对低廉、适应恶劣工作环境能力强等特点。

EPON相比工业以太网的优势在于：

① ODN中均为无源器件，可靠性强，布设容易。

② 网络建设成本低。

③ 网络扩容、扩展难度低。

而工业以太网的优势在于：

① 节点间传输距离更远，覆盖范围更大。

② 工业以太网交换机耐受恶劣环境能力强。

③ 可以采用环状网络等冗余拓扑结构，组网可靠性更高。

④ 数据传输的实时性更高。

综合考虑工业以太网和EPON的优劣可以发现，在电力终端通信接入网的技术选择中，EPON更适合高密度的人口集中区（A+、A类地区），工业以太网更适用于节点密度较低的市区或郊区（B类、C类地区）。此外，工业以太网还适宜布设在对数据实时性要求高的专用场景下。

无线专网的信号覆盖可以根据实际应用情况进行基站规划建设，使其信号得到保障，可以满足配网自动化、电能量采集、负荷管理及应急抢修检修管理等需求，主要适合于实现光纤不便于敷设部分（如直埋电缆等）的数据通信。在D、E类供电区域，以无线或载波通信方式为主。中小城区配电网有复杂的地理情况，可以使用无线专网使其适用于配电网生产实时性控制类及非控制类业务的需求。

6.3 适用场景分析

在合理选择城市模型的基础上，按照是否承载控制业务分场景对各种组网模式的技术、安全和经济成本进行对比分析。选择沿海某经济发达的中型城市为比较模型。其中城市中心区负荷密集、对供电可靠性要求很高的A+区域涉及电缆馈线50条，线路长度均在2km左右；市区负荷较为密集、对供电可靠性要求高的A类区域涉及电缆馈线60条，线路长度均在5km左右；负荷集中、对供电可靠性要求较高的B类区域涉及架空裸线120条，线路长度均在5km左右。上述各区域内的馈线全部采用“手拉手”接线，且满足N−1准则，每两馈线之间通过联络开关互联。此外，还有负荷较为集中、对供电可靠性要求中等的C类区域涉及架空裸线馈线180条，线路长度均在10km左右，且均采用辐射状接线，不满足N−1准则。各类馈线共计410条。规划中的计算参数均按典型参数选取，其中自动化三遥业务终端共计395个，配电自动化二遥业务终端共计780个；用电信息采集终端共计22.1万个；分布式电源终端共计100个；电动汽车充电站2个，电动汽车充电桩共计300个。

按照以上数据模型，建立以下三种通信技术覆盖场景进行技术经济比较。

场景一（仅承载控制类业务）：采用光纤专网或无线专网通信方式进行组网建设，覆盖区域为数据模型中的A+和A类区域，涉及馈线110条，只承载配电自动化三遥终端，接入终端数量共计215个。

通信性能要求：要求光纤专网传输速率≥19.2kbps，其他方式≥2.4kbps；遥控时延≤6s；配电自动化终端并发要求100%。

场景二（承载控制与非控制类业务）：采用光纤专网或无线专网通信方式，覆盖区域为数据模型A+、A、B类区域，接入A+和A区域内可与配电自动化业务共用通信资源的用电信息采集等非控制类业务终端以及B类区域内的配电自动化终端和可与配电自动化业务共用通信资源的用电信息采集等非控制类业务终端。涉及馈线120条，承载配电自动化终端数量共计420个，与配电自动化终端同站点的用电信息采集业务终端数量共计22155个、分布式电源业务终端共计70个。

通信性能要求：配电自动化系统要求光纤专网传输速率≥19.2kbps，其他方式≥2.4kbps；遥信时延光纤通信<2s，无线通信<30s；遥测时延光纤通信<2s，无线通信<60s；遥控时延≤6s；并发要求100%。用电信息采集传输速率按照要求自适应匹配，一般最低为1.2kbps，最高为40kbps；系统控制操作响应时间≤5s，常规数据召测和设置响应时间<15s；目前采用轮询机制，规定时间段内将数据上传至主站，无明确并发要求。10kV分布式电源终端单点接入的流量是42.3kbps，380/220V分布式电源终端单点接入的流量是1.05kbps；分布式电源遥控业务要求光纤时延≤10s，并发要求参照配电自动化及用电信息

采集业务。

场景三（承载非控制类业务）：采用光纤专网、无线专网通信方式，接入场景一和场景二以外所有配电自动化二遥、用电信息采集、分布式电源、电动汽车充电桩等非控制类业务终端。涉及馈线410条，承载配电自动化终端数量共计540个、用电信息采集业务终端数量共计199395个、分布式电源业务终端共计30个、电动汽车充电桩共计300个。

通信性能要求：光纤专网传输速率≥19.2kbps，其他方式≥2.4kbps；遥信时延光纤通信＜2s，无线通信＜30s；遥测时延光纤通信＜2s，无线通信＜60s；配电自动化终端并发要求100%。用电信息采集传输速率按照要求自适应匹配，一般最低为1.2kbps，最高为40kbps；系统控制操作响应时间≤5s，常规数据召测和设置响应时间＜15s；目前采用轮询机制，规定时间段内将数据上传至主站，无明确并发要求。10kV分布式电源终端单点接入的流量是42.3kbps，380/220V分布式电源终端单点接入的流量是1.05kbps；分布式电源遥控业务要求光纤时延≤10s，并发要求参照配电自动化及用电信息采集业务。电动汽车单个充电桩带宽要求为4kbps；系统时延要求＜5s；由于采用互联网承载，并发数量取决于互联网通道及服务器性能。

6.4 总　　结

本章对终端通信接入网的组网技术选型分析进行了介绍。首先对电力典型场景进行了分析，从各电力业务对包括网路容量和实时性在内的网络资源需求入手，结合各典型场景下的业务类型及配比，得出各典型场景下的终端通信接入网对网络覆盖范围、网络容量、实时性、可靠性等各种网络性能的需求。进一步地，针对光纤专网（包括EPON和工业以太网）、无线专网（包括LTE-230MHz及LTE-1.8GHz）等组网技术，分析技术特征，并对比各技术与各典型场景需求的匹配度，得出各组网技术的建议适用场景。

第7章
电力终端通信接入网运维技术



7.1 行业外运行监视与故障分析技术手段和应用效果

7.1.1 基于设备自身网管的运行监视技术

1. EPON设备网管

在网络管理领域，随着基于TCP/IP体系的网络管理技术的不断发展，SNMP已经成为事实上的标准。采用SNMP管理协议框架，对EPON网络实体资源实现有效管理已成为EPON设备主流的网络管理方式。

SNMP（简单网络管理协议）是一种基于TCP/IP的网络管理协议，它使用UDP作为传输层协议，能管理支持代理进程的网络设备。SNMP主要包括SMI（管理信息结构）、MIB（管理信息库）和SNMP协议几部分。SMI给出了管理对象定义的一般框架。MIB是设备所维护的全部被管理对象的结构集合。SNMP协议包括SNMP操作、SNMP信息的格式以及如何在应用程序和设备间交换消息。

EMS网管系统安装在工作站，与OLT设备之间通过带外网管接口或带内接口相连。EMS网管系统和OLT、ONU设备之间采用SNMP协议进行通信，实现在EMS中对OLT、ONU的统一管理。通信的方式有两种：

① 轮询。管理站每隔一段时间对所有OLT和ONU代理站的MIB进行主动查询，各代理站返回被查询的节点值。

② 告警（Trap）。当某些指定事件发生时，代理进程向管理站发送Trap报文。管理站接收、显示告警事件，并做相应处理。

同时，OLT设备和ONU设备具备本地Console接口，可以实现本地操作管理维护。

EPON网管系统按照网管功能基本可分为五大模块：拓扑管理、故障管理、性能管理、配置（资源）管理和安全管理。

拓扑管理：用于构造并管理整个网络的拓扑结构，用户通过浏览网络拓扑视图可实时了解整个网络的运行情况。拓扑管理中通过自动拓扑发现或手工增加拓扑节点来上载网络设备的拓扑数据，并支持拓扑设备的增加、删除、修改、查询操作。

故障管理：完成对所有被管理设备上报的告警，以及网管系统本身各模块在运行过程中产生的告警信息的处理，主要包括告警信息和运行信息的实时监控，查询设备的历史告警信息和运行信息，查询和配置设备的告警信息。

性能管理：对设备的行为以及网络和网络单元的有效性进行评估和报告。它的作用是收集统计数据，以便对网络、网络单元或设备的行为和有效性进行监视和校正，并帮助规划和分析。

配置（资源）管理：实现对EPON设备进行各种业务的配置与查看功能，如带宽分配、VLAN配置、QoS、ACL、IGMP等功能的配置与查看。同时，将所有被管资源分类显示和管理，包括设备、机槽、机盘、端口、纤缆、业务用户和业务用户组等信息。

安全管理：完成网管系统本身的安全控制。系统安全主要通过网管用户权限进行控制，用户在启动网管客户端后，需用已经建立的网管用户登录，并且只能在允许范围内执行该用户被授权可以执行的网管应用，即分权分域的管理模式。系统将记录用户对各个管理应用执行的敏感操作，管理员可以通过监视、浏览用户操作日志来取得系统的所有管理操作信息。

EPON网管系统的北向接口应提供登录、资源、拓扑、告警、性能统计、业务发放等功能，保证NMS访问服务的可扩展性、一致性和易操作性，保证EMS服务实现的多样性，不同设备、不同业务类型服务的易配置性。北向接口常采用的协议有CORBA、TL1、SNMP等。

2. 无线设备网管

目前，无线技术种类繁多，有无线公网的GSM、TD-SCDMA、GPRS，也有无线专网的WIMAX、McWill，但是无线网管系统都遵循统一的方案，即从终端网元节点开始，通过在无线网络结构中占据主控地位的汇聚网元节点汇聚管理链路，使用部署在汇聚节点近端的OMM（操作维护模块）系统对这些终端网元和汇聚网元进行管理，最后通过部署在专用设备上的EMS系统对来自各个OMM系统的信息进行汇总、处理，对外提供NMS的北向接口。

3. 工业以太网交换机设备网管

目前工业以太网交换机分网管型与非网管型，网管型以太网交换机通常提供了基于终端控制口（Console）的本地管理，以及基于SNMP、Telnet、Web等多种网络管理方式的远程管理。网络管理人员可以对该交换机的工作状态、网络运行状况进行本地或远程的实时监控，管理所有交换端口的工作状态和工作模式。非网管交换机相对于可网管交换机而言，是不能被管理的，不支持如监控交换机端口、划分VLAN、设置Trunk端口等管理功能，它对数据都是不做处理直接转发的。下面将只对网管型的工业以太网交换机进行分析。

由于基于EtherNet/IP的工业以太网控制网络是开放的体系结构，它基于成熟的IEEE 802.3和TCP/IP协议与标准，因此目前通常采用SNMP协议进行工业以太网的网络管理。

工业以太网交换机的管理系统按管理功能划分为网络管理和系统管理两部分。网络管理涉及网络相关的对象与参数。从图论观点，工业以太网可抽象为一系列节点间的无向图，节点代表设备，连接代表网络通信系统。网络管理中ISO规定的五大网络管理功能有网络拓扑管理、配置管理、性能管理（网络监控和设备状态监控）、故障管理和安全管理。

7.1.2 应用效果对比分析

设备网管系统在网管功能、标准规范、北向接口等方面的差异是非常大的，对比如表7-1所示。

表7-1 各种技术形态设备网管功能对比

	xPON	工业以太网交换机	McWiLL	中压PLC
主要网管功能	具备配置管理、告警管理、性能管理、拓扑管理功能	工业以太网交换机分网管型与非网管型，网管型具备配置管理、告警管理、性能管理、拓扑管理功能	具备配置管理、告警管理、性能管理、拓扑管理功能	大部分中压PLC没有网管，少部分的PLC网管采用私有协议，主要管理功能为告警、拓扑管理
网管功能标准	“基于以太网方式的无源光网络（EPON）系统第一部分：技术条件（报批稿）”中对EPON网元管理系统的管理功能作了要求	在国网企标“电力专用工业以太网交换机技术规范（报批稿）”与YD/T1099—2005 以太网交换机技术要求未对网管管理功能进行规定	未有相关标准规范McWiLL网管功能	没有
是否有北向接口	有	大部分没有	有	没有
北向接口协议	SNMP、CORBA、TL1、FTP等	SNMP	CORBA	私有
北向接口标准	YD 1664—2007基于以太网方式的无源光网络（EPON）网络管理接口技术要求，中国移动、中国电信都有EPON厂商网管系统北向接口规范	没有	没有	没有

从目前看，主要存在以下问题：

① 缺乏综合管理能力，综合网管系统的管理主要依靠设备网管系统，如厂家EPON网管、工业以太网交换机网管或厂家综合设备网管系统。各种设备网管系统都是独立的，只能分散管理厂家自己的设备，不能形成跨厂家的综合管理能力，各个厂家的管理系统兼容性差，形成了一个个信息孤岛，对提高管理水平极为不利。

② 部分网络设备缺乏管理系统。在配用电通信网络中很多通信设备不具备网管功能，如GPRS/CDMA通信终端、非网管型工业以太网交换机、中低压载波设备等。

③ 缺乏统一标准规范的北向接口，使得综合网管系统难以与厂家设备网管系统进行互联互通。

基于设备网管的运监技术通过标准化网管接口获取设备配置、告警和性能等数据。在网管系统建设思路方面，各运营商大同小异。综合网管系统都是以“集中监控、集中维护、集中管理”为运维管理的核心思想，一般都采取“省级集中”模式部署，并高度重视系统整合工作，发挥系统整体功能的优势。在网管系统功能应用方面，电信运营商在日常运维过程中一般极少涉及设备网管，基本上在综合网管系统中满足日常运维绝大部分应用的需要，相应的综合网管系统具有标准先行、功能闭环、资源多态、全路由管理、监控一体和自动派单等突出特点，但是在应用过程中存在以下问题。

（1）设备状态、流量状况缺乏监管

由于现有的网络管理系统基本是设备、网元级别的监控，存在监控粒度过细和业务资源抽象不足的问题，电信业务的实现通常是端到端的过程。以基本的短信业务为例，从用户终端发起，在接收用户终端终止，这个端到端过程涉及多个网元和连接。按照网元级别监控，得到的是网元的负载等指标，而从业务出发则更希望了解业务的实际状况。

（2）故障定位的局限

在定位故障过程中，根据电信运营商的实际经验，对于性能分析和控制，必须准确依托于资源数据，缺乏足够的资源信息，单纯依赖网管设备、网元级性能参数，很难向用户提供形象而准确的故障定位，更谈不上多故障的相关分析、关键故障的确认等能力。而且现有通信网络采用分层分级的模式建设和运维管理，现有各级网络设备并不完全统一，各厂家设备专业网管系统间并无故障告警信息的转递机制，对于跨越各级网络的业务或数据流，没有可快速进行故障定位和分析的专业系统和技术手段，造成故障定位和分析过程缓慢，较难定位。

（3）网络管理欠缺统一

现有电网数据网网管运行管理的支撑手段薄弱，只能管理本级的网络，不能支撑各级通信调度协同指挥，不能有效发现各级网络拥塞、泛洪，难以规避全网瘫痪的网络风险。现网中目前暂时没有针对实时流量监测、故障智能定位、故障智能分析、网络性能析、流量控制统一的管理系统。

正是由于存在以上问题，单纯的设备综合网管难以满足多层级网络高效故障诊断及定位需求，后续有必要研究基于流分析的检测及故障分析技术，攻克实时流量监测、故障智能定位、故障智能分析、网络性能分析、流量控制等关键技术，构建结构合理、安全可靠、可视的监控分析系统，以满足智能化、信息化电网管理理念的要求。

流量分析技术根据源IP地址、目的IP地址、协议号、源端口号、目的端口号等这样的几元组来定义流，或者说网络流被定义为由确定流的信息几元组（如源IP地址、目的IP地

址、协议号、源端口号、目的端口号这样的五元组）定义的由源到目的的单向数据包序列。通常认为具有相同的这几元组信息的网络信息属于同一个网络流。根据网络流量的处理方式，流量分类技术分为两大类：基于流的网络流量分析技术和基于非流的网络流量分析技术。

7.2 行业内运行监视与故障分析技术手段和应用效果

电力通信网主要分为通信骨干网和通信接入网两大部分，通信骨干网的网管系统相对比较成熟，但是通信接入网建设刚刚起步，并且包含多种通信方式，因此，通信接入网的网管系统相对比较复杂。网络接入业务是指以有线或无线方式提供的、与网络业务节点接口（Service Node Interface，SNI）或用户网络接口（User node interface，UNI）相连接的接入业务。通信接入网网络管理的结构模式在国际上主要分为 3 类：集中式网络管理、分级式网络管理和分布式网络管理。电信网随着光纤通信接入网的快速发展，接入网最终使用国际 V5 标准接口的开放式系统，使原有的封闭的交换机用户接口成为标准化的开放型接口。在引入接入网后，现有端局在原有意义上的数量减少，中继网原有中间层级减少，网络复杂程度也不断降低，随着业务节点容量的持续增加，逐步形成一个无极的动态接入网网络。配电自动化系统的通信接入网建设方案建议采用多种（EPON、中压载波、无线专网、无线公网、GPRS/CDMA/3G 等）通信方式相结合的原则组建配电通信网，提出通过构建“配电一体化通信平台”实现多种通信方式“统一接入、统一接口规范和统一监测管理”，确保通信通道安全、可靠、稳定运行，并给出了各种通信技术的建设典型方案。统一接入有效融合了多种通信方式，为配电自动化系统提供综合的接入解决方案，配电主站设备通过统一接口规范连接到配网通信综合接入平台。

目前接入网综合网管理仍处于起步阶段，缺乏标准和实际经验，没有统一的接入网网管国际标准。电力系统的通信网网络管理起步较晚，考虑到电力通信网特别是配用电通信网网络结构复杂、通信方式多样、通信终端种类繁多且覆盖面广，管理难度非常大，因此需要采用分布式网管体系，其优点是灵活性强、成本低。目前电力通信接入网的多样性适合窄带及宽带多业务接入网的网络系统，便于网络升级。

世界各大公司都支持分布式网络管理模式。当前分布式网络管理模式框架一般采用的管理模式主要有公共对象需求代理人结构（Common Object Request Broker Architecture，CORBA）、分布计算环境/分布管理环境、分布式公共对象模型（Distributed Common Object Model，DCOM）等，但是 CORBA 在国际上仍被优先推荐和采用，其分布结构对象和框架的运用使得它可以采用不同供应商的产品并跨越不同的操作系统和网络。此外CORBA还可以对所有对象实施操作而完全不必知道它们采用何种语言以及它们所处的位

置，这一优点使其能够在未来复杂的通信信息网络中发挥极其重要的作用。我国电力系统行业已经开展适于分布式网管系统的 CORBA 等框架结构的研究，并且正在开展相关系列标准的制定工作。

由于目前国内大多数供货商采用各自不同的技术研制了很多专业网络管理系统，这些专业网管之间缺乏共同的体系结构，存在管理信息不能互通、协议不兼容等问题。需要建立支持混合通信网络环境下的综合网络管理、网络运行监控及优化、业务调度的统一的综合网络管理系统，称为统一的综合配网网管系统。目前统一的综合配网网管系统与厂商网管系统间接口有两种处理方式：

① 由统一的综合配网网管确立接口，保持统一界面风格，各厂商按照统一规范要求开发。其优点是接口统一，统一网管开发速度快，缺点是每个厂商的开发工作量较大，与各厂商密切配合实施的难度大。

② 统一综合网管系统直接使用各厂商目前提供的北向接口CORBA、可扩展标记语言（Extensible Markup Language，XML）、TL1、Java 远程方法调用（Remote Method Invocation，RMI）、远程过程调用（Remote Procedure Call，RPC）、简单网络管理协议，对各厂商原有的系统网管无须改动。其缺点是各厂商虽然提供了北向接口，但在表现形式上还是多种多样的，人机交互界面也不统一，而统一的综合网管则要开发各种接口与各厂商的网管系统适配。从系统总体的开发时间和建设成本看，后者（即统一综合网管系统继续使用各厂商原有的接口）要优于前者。

配网通信接入层采用光纤 EPON、中压载波、无线专网、无线公网 GPRS/CDMA/3G 等多种通信方式相结合的原则组建配电通信网，并且在配电主站端配置配网通信综合网管系统，实现对EPON、中压载波通信、电力无线专网和无线公网GPRS/CDMA/3G/TD 等的配网通信设备、通信通道、重要通信站点的工作状态统一监控和管理，包括拓扑管理、故障管理、性能管理、配置管理、安全管理等。一般采用分层架构体系建设配网通信综合网管系统，统一的综合配网网管系统与厂商网管系统间接口采用基于 RMI 技术的北向接口实现。

目前，配用电通信网运维管理的有序和高效需求也日益明显。因此，进行配用电通信网业务故障检测与定位技术的研究，并开发配用电通信业务故障监测系统将极大地推进配用电通信网络管理信息化建设的进程，为配用电通信网管理提供统一的平台，实现配用电通信网的“统一管理、综合监视、集中调度、汇总分析、优质服务”，对保障电网配用电通信网的安全可靠运行、通信资源整合优化、服务质量提升，以及推动配用电侧电网智能化进程等方面具有重要意义。

7.2.1　基于载波设备的网管技术

PLC设备可分为可网管型和不可网管型两种，大多数PLC设备无网管功能，即使存在

设备厂家网管，各厂商在PLC设备与网管通信协议上也较多地使用私有协议。

设备厂家网管按照网管功能基本可分为网络拓扑管理、设备管理、设备监控（网络监控和设备状态监控）、告警管理、安全管理等五大基本模块。但对于各种网管功能，PLC厂家网管支持得并不是很完善，比如：

① 将从载波机添加到拓扑视图中只能通过手工方式完成，所以可以支持所有组网方式。但对于手拉手组网方式厂家网管的拓扑显示和设备状态显示是有问题的，不能正确显示从载波机的连接和使用状态。

② PLC设备的离线告警信息是完全依靠网管轮询实现的，没有设备主动上报功能，所以在实时性方面相对差些。

③ 从载波机设备状态依靠网管轮询实现，轮询方式也较为多样，常见的有：

- 采用基于模型的推理（Model-based Reasoning）技术对PLC网元设备进行有效管理。即设备厂家网管向配电终端发送某种数据采集请求，若配电终端通信正常运行，就可以判定该配电终端所接入从载波机工作正常；反之，如果该配电终端通信不正常运行，而其相邻的配电终端正常运行，则可以认定该配电终端所接入从载波机出了故障。
- 采用直接查询PLC网元设备状态的管理方式。即设备厂家网管向主载波机发送设备状态查询请求，主载波机收到请求后，以广播的方式查询其下挂从载波机的设备状态，主载波机获取从载波机设备状态信息后对网管的查询请求进行回复。

7.2.2 基于综合网管的运行监视技术

在配用电通信综合网管方面，随着近几年配电自动化、用电信息采集、电力光纤到户、智能用电小区等试点的大量建设，配用电通信与网络管理逐渐成为关注的焦点。目前配用电通信综合网管的研究与建设一直处于落后状态。从各地区试点情况来看，配用电通信的网络管理主要是以厂家设备网管为主，如EPON设备网管、工业以太网交换机设备网管、McWill设备网管等。

1. 综合网管需求分析

在电力通信网中，配电和用电环节由于过去自动化程度较低，因此发展相对滞后。电力通信网具有分布广泛、终端节点众多、承载业务类型丰富多样、多种接入技术混合应用、现场运行环境恶劣的特点，随着电力通信网的大规模建设，电力通信网络的管理、维护等工作更加复杂和困难，因此建立体系完善、运行可靠的可管理、可维护的通信管理系统具有重要意义。

1）运行维护需求

随着公司集约化管理、信息通信一体化建设的推进，电力通信网运行维护管理体系规

程也需要与公司接入网的实际运维方式相结合，梳理出电力通信网运行管理规范。

2）功能需求分析

依据电力通信网建设现状、业务与运维需求，电力通信网综合网管系统应满足以下功能需求。

（1）通信实时监视：指整合、处理和分析设备网管至综合网管系统的各种告警信息和性能信息，实现在统一的界面下对多厂商设备运行状态的集中监视，实现面向网络、面向业务的告警管理以及故障分析处理手段。主要功能模块包括告警集中监视、网络运行状态监视、故障分析与处理、性能管理。

（2）通信资源管理：应提供对通信网络各种通信资源数据的规范、常态管理功能，实现面向通信网络、通信设备、通信业务等各类通信资源的规范化管理，使资源的使用更加便利、资源数据的查询更加准确，并为通信资源的建设和规划提供依据。通信资源管理主要包括资源信息管理、配置管理、资源图形管理、资源查询统计分析和资源预警分析等功能。

（3）通信运行管理：通信运行管理类应用从通信运行的值班调度、方式、检修、故障、备件等方面的流程化管理角度定义相关功能，对各类工作的流程化、标准化、信息化进行管理。通信运行管理功能主要包括运行值班管理、通信运行方式管理、通信检修管理、缺陷故障管理、备品备件管理等。

电力通信接入网系统功能在资源管理、实时监视、运行管理等三大应用与骨干通信网综合管理系统类似，但在管理对象、拓扑呈现、运行方式管理、配置管理等方面存在较大差异，下面针对不同需求进行阐述：

（1）资源管理。综合网管系统管理设备类型包括EPON、工业以太网交换机、PLC、无线设备等，由于管理设备间存在较大的设备属性差异，因此在资源管理部分需根据设备的类型进行资源信息的管理、查询和统计。另一方面，受限于配网架构、不同业务需求、光缆已辐射到的位置、设备放置条件等多种因素，接入网在实际组网中存在大量混合组网的情况，对综合网管系统在图形拓扑管理功能上提出了更高的要求，如在一张拓扑图中呈现多种连接方式、拓扑图分层显示等功能需求。

（2）实时监控。由于综合网管系统的下层接入对象存在无主动上报告警功能的设备或设备网管，因此部分设备或设备网管需综合网管系统以告警轮询的方式获取告警信息，直接导致综合网管系统在实时监视的性能上有所下降。

（3）运行管理。由于骨干网是四级调度、分级管理的运维管理模式，而接入网的调度、运维模式层级较少；另一方面，接入网的业务开通方式与骨干网的业务开通方式也存在较大差异。因此在检修管理、运行方式管理、缺陷故障管理等方面与骨干网将有所差异，运行管理流程需根据管理制度重新梳理。

3）系统互联需求分析

（1）实时监视纵向互联需求

设备实时告警：综合网管系统可通过纵向互联接口将设备实时告警发送至上级综合网

管系统，上级综合网管系统也可通过纵向互联接口获取综合网管设备实时告警信息。

网络拓扑：综合网管系统可通过纵向互联接口将网络拓扑发送至上级综合网管系统，上级综合网管系统也可通过纵向互联接口获取综合网管网络拓扑信息。

（2）资源管理纵向互联需求

设备台账：综合网管系统可通过纵向互联接口将设备台账发送至上级综合网管系统，上级综合网管系统也可通过纵向互联接口获取综合网管设备台账信息。

设备运行指标：综合网管系统可通过纵向互联接口将设备运行指标发送至上级综合网管系统，上级综合网管系统也可通过纵向互联接口获取综合网管设备运行指标信息。

（3）运行管理的纵向互联需求

检修流程：对于检修流程中涉及的需要上级单位审核或者下级单位配合的步骤，系统能够通过纵向互联接口进行流程和表单流转。

故障（缺陷）流程：对于故障流程中涉及的需要上级单位审核或者下级单位配合的步骤，系统能够通过纵向互联接口进行流程和表单流转。

方式流程：对于方式流程中涉及的需要上级单位审核或者下级单位配合的步骤，系统能够通过纵向互联接口进行流程和表单流转。

（4）横向互联需求

与GIS的横向互联描述：电网GIS空间信息服务平台为通信管理系统提供GIS空间信息，确保通信空间基础数据的一致性。

与PMS的横向互联描述：对于设备检修、缺陷故障等信息，需要发布到PMS系统，为电力生产相关部门提供数据依据。

与配电自动化系统/用电信息采集系统的横向互联描述：将通信网络的实时及历史状态传送到配网应用系统中，为配电自动化系统/用电信息采集系统等相关系统的可靠运行提供保障。

2. 北向接口技术

在网络管理系统中，北向接口是一个重要的模块。从总体概念上来说，北向接口是下层系统对上层系统提供的接口。

1）CORBA

CORBA是一个分布式的架构规范，而且它是面向对象的。它诞生于20世纪80年代末，由对象管理组（Object Management Group，OMG）提出，在20世纪90年代逐步趋于完善。提出CORBA的目的是为了解决开发费时而复杂的分布式对象应用。CORBA为了便于共享和重用，使用了面向对象的方法来实现软件，实现了一次开发多次使用的功能。CORBA只是OMG支持的一个工业标准，而且目的是为了实现分布式计算。CORBA可以用于解决远程对象之间的互操作问题。微软公司的DCOM也致力于解决该问题，然而它在Windows平台上实现得更好，在其他的操作系统上不尽如人意。而CORBA是真正

具有平台独立性的，且CORBA还具有语言独立性的特色，也就是说客户端和服务器端可以分别使用Java和C++或者其他语言来实现，它定义了接口定义语言（Interface Definition Language，IDL）来实现这种语言独立性。因此，可以说CORBA是一种具有平台独立性和语言独立性的面向对象的互操作模型。

CORBA的特点如下：

（1）CORBA的平台无关性实现了对象的跨平台引用，开发人员可以在更大的范围内选择最实用的对象加入到自己的应用系统之中。

（2）CORBA的语言无关性使开发人员可以在更大的范围内相互利用别人的编程技能和成果，是实现软件复用的实用化工具。

CORBA的底层结构是基于面向对象模型的，由3个关键模块组成：

（1）OMG接口描述语言（OMG Interface Definition Language，OMG IDL）。IDL是一种描述性语言而不是程序设计语言，只描述接口和相关的数据类型，不描述实现，独立于编程语言，但可以映射为多种编程语言，目前有C、C++、Java、Ada、COBOL和Smalltalk。应用时由IDL编译器来实现从IDL语言到具体编程语言的映射。

（2）对象请求代理（Object Request Broker，ORB）。CORBA的核心是对象请求代理ORB，它提供对象定位、对象激活和对象通信的透明机制。客户发出要求服务的请求，而对象则提供服务，ORB把请求发送给对象、把输出值返回给客户。ORB的服务对客户而言是透明的，客户不知道对象驻留在网络何处、对象是如何通信、如何实现以及如何执行的，只要他持有对某对象的对象引用，就可以向该对象发出服务请求。

（3） IIOP标准协议（Internet Inter-ORB Protocol，也称网络ORB交换协议）。

基于CORBA网络管理接口协议栈采用TCP/IP协议族，并在其上实现IIOP。

2）TL1

TL1由Telcordia（先前的Bellcore）定义，全称Transaction Language-1，是一种ASCII型的人机（man-machine）交互协议，也是一种标准的电信管理协议。

TL1是电信领域（尤其是在北美）广泛使用的一种管理协议。它能够管理多种宽带网和接入网，包括SONET/SDH，ATM（Asynchronous Transfer Mode）。TL1得以在世界范围流行的主要原因是：和其他的协议相比，它很容易实现和维护。TL1报文有一种很好的，甚至用户和操作者都能设计和理解的结构化格式。之前，传统命令行接口（Command Line Interface，CLI）成为大多数设备（网络设备或电信设备）厂商必须提供的完整的接口，管理这些设备的唯一方法就是通过串口连接，发送命令。这使得TL1更加流行，并使得CLI在电信领域成为首选。

TL1的特点如下：

① TL1是一种标准CLI接口。与其他的CLI接口相比，TL1遵循约定的语法，不同的命令具有固定的格式。

② TL1是一种ASCII文本格式的人机语言，因此开发人员和操作者都能够望文知义。

③ TL1的消息容易阅读，所以TL1不需要复杂的调试和协议分析器。用户看到的就是TL1所表达的。

④ TL1具有延时激活（Delayed Activation）的功能。延时激活是指请求消息可以被缓存在网元中，稍后才实际被执行，这种执行可以在指定时间主动执行，也可以被TL1消息主动提前执行，当然也可以取消执行。

⑤ TL1具有主动上报功能。通过主动上报，网元可以将当前的性能、告警或其他用户感兴趣的事件实时、主动地上报给用户，用于监视网元的实际运行状态。

⑥ 具有消息的确认机制。TL1定义了一种acknowledgment消息，可以对输入的命令消息进行简短的应答确认。比如，如果一个TL1输入消息在网元中运行的时间超过2s（也即2s以后网元才会对输入消息作出响应），就可以提前对这个输入消息生成一个acknowledgment消息，告诉用户：您的输入消息正在被处理之中。

从应用上讲，TL1北向接口主要面向的是运营商的业务发放。由于网管软件提供了很多不同业务的配置，包括了宽带、窄带、语音等不同模块的业务配置功能，而传统网管前台界面中不同业务所需要配置的操作流程千差万别，运营商往往需要一个命令行配置接口来进行相应的业务发放功能。TL1北向接口作为一种方便易懂的自治消息接口，是使用最多的用于业务发放的北向接口。

3）XML

XML是表示结构化信息的一种标准文本格式。XML因具有良好的数据存储格式、可扩展性、结构化等特点而被用于网络管理接口。但是，由于XML仅仅是对数据的定义，本质上停留在接口描述层，所以虽然XML提供了一种结构化或可扩展描述信息的方式，但是要成为功能完全的网络管理系统的一部分，还需要底层通信协议的支持。XML技术本身是不绑定任何协议栈的，可以根据需要灵活选择底层协议。W3C推荐使用基于HTTP/SOAP的协议栈。

相对于其他网络管理接口，XML描述的信息格式通用性更强，受到软件提供商的广泛支持，易于进行信息的交流与开发。另外，XML易于异构网络管理系统间数据的共享和交互，XML独立于平台、独立于底层协议、独立于语言。

4）SNMP

SNMP（简单网络管理协议）是一种基于TCP/IP的网络管理协议，它使用UDP作为传输层协议。SNMP主要包括SMI（管理信息结构）、MIB（管理信息库）和SNMP协议几部分。SMI给出了管理对象定义的一般框架和SNMP报文的描述规则，它是构成整个SNMP的基础。MIB是管理对象结构化组织的一种抽象。它是一个概念上的数据库，由管理对象组成，描述了SNMP所有用到的管理信息库的结构及其中变量的定义，以树形结构表示。SMI和MIB都是采用OSI的ASN.1（抽象语法表示）定义的。SNMP协议提供在网络管理站和被管理代理之间交换管理信息的方法。网络管理站通过查询或监听陷阱的方法获取被管代理站的信息。

SNMP是一个异步式请求/响应协议，SNMP实体不需要在发出请求后等待响应，因此在计算机网络中应用非常广泛，成为事实上的计算机网络管理标准。由于SNMP相比较CMIP来说在实现上有比较简单，使用者众多的特点，做电信网络设备也逐渐部分地采用SNMP协议作为网络管理接口。但SNMP有许多自身难以克服的缺点：

① 不适合大型网络管理。因为SNMP基于轮询机制，这种方式有严重的性能问题，所以不适合查询大量的数据。

② SNMP的Trap是无确认的，这样有可能导致非常严重的告警无法确保发送到管理者，安全管理较差。

③ 不支持如创建、删除、动作等类型的操作，要完成这些操作，必须用SET命令间接触发。

④ SNMP的MIB模型不适合比较复杂的查询。

基于SNMP网络管理协议栈采用了TCP/IP协议族，传输层协议主要采用了UDP协议，TCP协议作为可选。在安全性方面，SNMPv3以下的版本使用了IPSec，属于网络底层通用安全机制，而SNMPv3使用了USM，USM是专为SNMPv3定义的一种安全模型，用于提供SNMP消息层的安全。

5）文件接口

当需要与网元传送大量的数据的时候，通常采用文件接口。在网管系统中通过文件接口传送数据量比较大的性能文件和配置文件。

文件接口基于文件传输协议，如FTP、TFTP、FTAM等。FTP（File Transfer Protocol，文件传输协议）是最平常的TCP/IP应用，我们通常使用的FTP服务都遵循RFC959。FTAM是一种基于CMIP/OSI协议栈的文件传输协议。TFTP接口没有安全认证机制，相对控制协议比较简单，程序比较小，在网络管理中经常用于文件传输。

3. 网络管理接口适配器

以下是对网络管理适配器的典型功能、管理范围、接入能力等相关内容的分析。

1）系统用途

网络管理接口适配器系统用途如下：

① 适用于多厂商网络环境下综合网管系统工程中各厂家网络管理接口的引接，同时适用于设备厂商根据规范提供标准的北向接口。网络管理接口适配器可以屏蔽不同厂家网管接口协议、信息模型和功能的差异性，使被管网络提供的网络管理接口统一，实现网络管理系统与被管网络之间的快速互连互通互操作。

② 能够适配多种网络管理接口协议并向上层网管系统提供统一网络管理接口协议，轻松实现被管网络和上层网管系统的互连。

③ 能够按照统一网络管理信息模型进行数据管理，屏蔽厂家差异，使上层网管系统管理更简单。

④ 能够提供性能、配置、告警等多方面的管理功能，满足上层网管系统的管理要求。

2）典型功能

网络管理接口适配器典型功能如下：

① 接口协议适配功能：提供对各设备厂商Q3、CORBA、TCP/IP、TL1、RS-232、FTP、SNMP以及数据库接口等不同网络管理协议进行适配，向上层网管提供统一的、符合规范要求的网络管理接口协议。

② 接口信息模型适配功能：屏蔽各设备厂商提供的接口信息模型的差异，遵循行业网络管理技术规范，归一化管理信息模型，使上层网管通过统一的管理信息模型对所有厂家的设备进行统一管理。

③ 接口功能适配功能：在协议和模型适配的基础上，遵循行业网络管理技术规范，提供统一的北向接口功能实现，满足上层网管包括配置管理、性能管理、告警管理和操作维护等在内的管理需求。

3）管理范围

网络管理接口适配器可管理范围如表7-2所示。

表7-2 网络管理接口适配器管理范围

序　　号	网 络 类 型	设 备 类 型
1	传输专业	WDM、SDH、PDH、MSTP、ASON
2	数据专业	ATM、DDN、IP
3	交换专业	PSTN、SS7
4	移动专业	GSM、CDMA、WCDMA、TD-SCDMA、CDMA2000
5	接入专业	ADSL、GPON、EPON、PDH
6	业务系统	MMS、SMS、IN、WAP、IVR
7	动力环境等其他专业	空调、电源、温度、湿度、水浸

4）接入能力

网络管理接口适配器具备和目前各专业网络大量设备厂商的接入能力，支持从厂家标准OMC北向接口、厂家私有OMC北向接口、设备直连接口的接入；支持的接入技术包括CORBA、TL1、SNMP、DB、TCP/IP、FTP、WebService等。

4. 基于单技术体制综合网管的运行监视技术

对于单技术体制的电力通信接入网而言，其综合网管系统主要基于北向接口协议实现。

依据设备厂家网管北向接口所采用的较为常见的通信协议，可知每种协议在不同的数据大小、交互方式等不同的要求下，其优势也各有不同。因此，在后续进行的终端接入网系统与底层厂家网管系统对接时，定义采用的通信协议也不应是单一类型，需要根据实际交互数据类型与交互方式综合考虑。建议如下：

① 业务发放、历史告警信息、资源信息、拓扑信息等采用TL1或CORBA协议。

② 实时告警信息采用SNMP或CORBA协议。

③ 性能数据采集采用FTP协议。

终端接入网系统的接口层应包含接口适配器层，将各种接口协议、各厂家的接口差异在适配器层予以消除，向上提供统一的数据模型。

其他需满足的要求如下：

① 接口应采用开放的标准化协议，以便接口的互联互通，并降低网管系统的开发成本。

② 接口信息模型应基于国际上通用的信息模型，以便多厂商网管系统的设计和开发。

③ 该接口向上提供的管理信息应该是完备的，足以提供多厂商网管系统所需的各种网络信息，支撑多厂商网管系统的开发。

④ 接口应该是相对稳定的，不应随着网管系统版本的升级频繁更改原有的协议和模型。同时接口应该具有一定的可扩展性。

5. 基于多技术体制综合网管的运行监视技术

对于多技术体制的电力通信接入网而言，配用电通信网络环境的复杂性决定了在网运行设备的多样性。除了光通信设备EPON、工业以太网交换机外，还有无线专网设备和PLC设备。在综合网管中要考虑多种设备类型融合管理的问题，对设备、端口属性中的差异需要特别关注。

由于电力通信接入网络接入设备的多样性，每种接入设备又存在多个厂家共存的情况。那么接入网管理系统必然面临接口协议的多样性和相同类型数据的差异性，这就要求在接入网管理系统中的数据采集平台具备针对各种设备、各个厂家的接口适配层，在接口适配层完成各种数据的差异化处理，最终符合接入网管理系统中对各种数据的定义及要求，形成统一的数据格式进行入库处理。接入网管理系统的接口适配层建议支持：

① 接入技术CORBA、TL1、SNMP、DB、FTP等。

② 接入专业EPON、工业以太网交换机、PLC、无线专网等。

③ 接入主流厂家，如华为、中兴、西门子、烽火、瑞斯康达等。

此外，由于中低压接入网网络环境相对复杂，根据各地区网络建设的差异，存在多种组网方案并存或混合组网的情况，这直接体现在接入网综合网管中拓扑呈现的复杂性和多样性上。

受不同配网架构、不同业务需求、光缆已辐射到的位置、设备放置条件等多种因素的影响，电力通信接入网中各种技术的混合组网方式比较常见，主要包括以下几种：

① 光纤（EPON、工业以太网交换机）+载波方案。

② 光纤（EPON、工业以太网交换机）+无线专网方案。

在接入综合网络管理系统中，对于以上两种混合组网方案进行分层管理。比如混合组网方案为EPON+载波：OLT设备放置在110kV变电站，光纤仅铺设到开闭站，ONU放置

在开闭站，同时在开闭站放置主载波机，从载波机放置在环网柜、柱上开关、配电室等地。那么在第一层拓扑视图中仅展示EPON层次的相关拓扑连接，EPON的拓扑呈现可参加EPON方案。若ONU下挂了主载波设备，那么在该ONU下的第二层拓扑视图中展示PLC层次的相关拓扑连接，PLC的拓扑呈现可参见PLC方案。

③ 光纤（EPON、工业以太网交换机）+公网组网方案。

在接入综合网络管理系统中，对这种组网方案只管理到专网的光纤接入设备层次，对于公网设备、公网告警等信息无法进行统一管理。专网的光纤接入设备的管理参见前面已介绍过的EPON方案或工业以太网交换机方案。

7.2.3 基于业务流量的流量分析技术

1. 基于非流的流量分析技术

基于非流的网络流量分析技术包括基于SNMP的网络流量分析方法、基于网络探针的网络流量分析方法和基于抓包的流量分析方法。

1）基于SNMP的流量分析技术

基于SNMP的网络流量分析技术主要是针对网络设备端口进行分析，这种技术依赖于对交换机、路由器等设备中SNMP MIB信息的采集来完成流量分析。

SNMP属于一种内部通信协议。要收集设备的信息、参数、运行状态等参数，都可以通过 SNMP 功能来完成。SNMP 具有以下技术优点：

（1）基于 TCP/IP 标准协议。

（2）自动化网络管理。

（3）对不同厂商产品的统一管理。

（4）报文种类少，易于第三方调用。

（5）SNMPv3 还提供了加密认证、用户访问控制等安全机制。

SNMP 网络架构由三部分组成：NMS、Agent 和 MIB。NMS 可以对网络设备或其他设备进行监控，并且能够主动向设备发送修改请求或者运行状态。Agent 则是对设备信息进行维护，把管理数据传递给发送请求的 NMS，属于一种应用模块。当存在设备故障或者变化时，Agent 将主动告知 NMS，即将查询或修改结果（Trap）发送给 NMS，及时更新设备的状态信息。被管理对象的各种属性是由MIB 定义的，如名称、访问权限和数据类型等。每个 Agent 都有自己的 MIB。

SNMP 的操作主要有Get、GetNext、Set、Response 和Trap，当前四种操作执行时，设备利用 161 端口、UDP 协议发送报文，而利用 162 端口、UDP协议发送报文来执行 Trap 操作。

基于SNMP的网络流量分析技术实现比较简单，结构统一，但是只能提供带宽利用率

等粗粒度指标，不能分析网络利用的具体细节信息，需要定时向网络设备发送SNMP。这些请求也给网络带宽和网络设备性能造成很大影响。由于采用轮询的方式获取信息，所以对实时性有一定限制。

2）基于网络探针的流量分析技术

基于数据采集探针的网络流量分析技术是指利用软硬件探针设备，从网络中获取原始数据报文，报文由专用的探针设备进行处理分析，从而获取网络流的各种信息，达到分析网络流量的目的。

硬件探针也是目前主流的流量获取设备，它通过串接或者旁接在设备或链路中获取网络流量，将进出设备或端口的流量传递给分析服务器。它具备强大的网络流量捕捉能力，可以将网络流量捕获并直接存储到硬盘上，流量存储的性能可以高达 1800Mbps，并可以提供全七层协议解码能力。

硬件探针的采集方式主要有分光部署和镜像部署。

（1）分光部署。

光分路器是将两台交换机连接的链路分割一部分光源给第三方接入设备，在保证原有链路数据传输的情况下，提供其他分析设备做数据采集。通常，光分路器将链路 Rx、Tx 方向的数据直接通过分光口输出，因此分光口的两根光芯上都有数据，分别对应链路的 Rx、Tx 方向数据，流量采集探针只需要将单条光芯接入到模块上即可。

（2）镜像部署。

交换机具备镜像端口功能，即将某个或者某几个端口的数据流量通过命令复制到指定的端口，该端口不支持通信功能。镜像端口的接口类型不限于光纤接口，也可以是 RJ-45 接口。通常一台交换机能够做两组镜像（session），被镜像接点可以是多个，但是每组镜像的镜像端口只能是一个。值得注意的是一般情况交换机的接入端口都是千兆级，千兆级镜像端口的带宽只有1Gbps，如果被镜像端口的数量较多，被镜像端口的总带宽很可能超过1Gbps，将会使镜像端口的流量过高，出现数据丢弃情况，影响分析的准确度。

探针采集系统一般由硬件探针（Probe）、管理服务器（Server）和数据分析程序（Analysis Application）三种组件构成。

（1）硬件探针。

硬件探针是利用分光或镜像端口进行数据分类、过滤，上传汇聚致中心服务器的数据库进行存储以及便于统一调用。

（2）管理服务器。

管理服务器由流量采集、管理程序和数据库构成。流量采集程序可以收集各个探针提供的数据流，并且对数据流进行解包，统计汇总，将数据存储在数据库中。探针与采集服务器利用特有的通信协议进行数据传输，并且采用主动上报的方式，一般采用安全性较高的 UDP作为传输协议。管理程序则采用了 TCP 专门的高层通信协议对探针设备和策略进行管理，可以直接对探针进行监控指标及维护策略下发；数据库可以满足对结构化数据的

存储，并提供分析查询及搜索操作。

（3）数据分析程序。

该程序可以按照任意条件从数据库中提取关注的数据信息，从而方便地为统计报表、图表提供相关的统计信息。

探针采集系统部署方式主要包括：

（1）旁接方式。

在这种模式中，数据流通过分光、镜像等方式复制并传递到流量分析系统相关模块，该模块作为整个系统的入口开始对数据进行处理。

（2）串接方式。

串接方式就是将设备串接在网络设备之间的通道上，位于广域网区域出口之间。优点在于流量控制比较简单，通常情况下，只要能够检测到协议流量，就可以采用丢包等方式达到控制流量的目的，节省大量的人力和时间成本。其缺点在于存在网络处理瓶颈。

（3）联动方式。

利用联动部署方式，通过利用两个物理设备进行功能分析和设备控制，其中一个设备负责流量的镜像，另一设备通过旁接的方式对数据进行分析。

基于数据采集探针的网络流量分析技术准确率高，实时性好。基于探针的网络流量分析方法的实现需要软硬件结合，对硬件要求较高，并且价格昂贵，部署复杂。

3）基于网络捕获的流量分析技术

基于数据捕获的网络流量分析技术指采用网络数据的捕获得到网络流量数据，其性能依赖于数据捕获的速度和效率。当网络设备不支持SNMP协议时，可以使用数据捕获的方式进行网络流量分析。

基于数据捕获的网络流量分析技术处理能力是有限的，在高速的网络下，会存在丢包以及数据包获取速率低等问题，但是其设备适应性较强。

2. 基于流的流量分析技术

基于流的网络流量分析技术目前比较成熟的流量采集方案有几种，由InMon、HP和Foundry Networks联合开发的sFlow，由思科开发的NetFlow，以华为/华三公司开发的NetStream等，另外IETF正在制订IPFIX（IPFlow Information Export）规范，这项规范为网络中流量统计信息提供统一的格式。

1）基于Netflow的流量分析技术

Cisco 公司提出能够实现测量和统计 IP 数据流的包交换技术 NetFlow。NetFolw是一种的基于流（flow）的网络流管理和分析技术。这项技术提供了一系列高效的服务，其主要功能包括网络流计数、网络规划、基于使用的计费，以及服务监控等。NetFlow通过处理数据流的首个IP包，生成缓存数据，以此来统计后续的数据包的信息。

2）基于Netstream的流量分析技术

这是H3C 公司提出的一种针对网络流量的统计技术和网络优化的技术，该技术能够对网络的流量进行多维度的分析和统计。NetStream与Cisco公司的NetFlow技术类似，通过流的概念对网络中的流量情况进行分析和统计。

NetStream 的功能包括：

① 计费依据：Internet 服务提供商和企业客户可以利用此功能来帮助计费，以便有效利用企业的资源。

② 网络规划：比如整个广域网骨干网络流量情况，通过流量统计从而提出对网络的调整和优化，实现低成本产生高效能。

③ 网络监控：如需要分析各种业务占用出口带宽的情况，可在广域网或者公网的出口设备中打开NetStream功能，通过对数据流的分析，并结合健康指标来判断网络的运行情况，及时发现网络架构合理与否。

④ 用户监控和分析：对于用户使用网络带宽及应用系统的情况，也可以利用NetStream技术来监控和分析，从而更好地分配网络带宽资源，满足用户的需求，提高网络的可靠性。

NetStream支持二层报文、IP报文（UDP、TCP、ICMP 报文）和MPLS报文的统计。对于IPv4报文，IPv4 NetStream会根据IPv4报文的目的IP地址、源IP地址、目的端口号、源端口号、协议号、ToS、接口输入/输出来定义流。对于IPv6报文，与IPv4报文不同的是增加了流量分析、流标签、输入接口或输出接口等来定义流。对于MPLS报文，用MPLS标签栈和IP信息共同定义数据流。

NetStream系统包含NDE、NSC和NDA三部分。NDE负责网络流分析处理，它会对网络设备中抽取的相关流数据进行统计，发送给NDA（NetStream DataAnalyzer）设备。NDE的报文是由NSC来负责解析的，将解析到的统计数据放到数据库中，由 NDA负责调用并解析，NSC通常作为运行在Windows中的程序存在。NDA从NSC中得到设备参数数据，并生成报表，可作为业务分析的依据。

NetStream关键技术有：

（1）流老化。

NetStream能够通过流老化方式输出流的统计信息，而NetStream缓冲区保存着流统计的数据信息。一旦流信息老化时，设备中的流信息输出数据将发送给NSC。因此，NetStream流老化有三种方式：按时老化、强制老化、TCP的FIN和RST报文触发老化。

（2）流输出。

流输出为了保存这些统计信息，会使设备的CPU占有率提高，同时也会加大网络中的带宽使用率，而且还会产生大量的数据占用设备存储介质空间。流输出包含普通流和聚合流两种，其区别是向NSC发送的数据流有无通过聚合关键项统计。

（3）NetStream采样过滤功能。

IPv4 NetStream可以与Sampler采样器配合使用，既减少了统计的报文数量，又保证了反映整个网络流的状况准确性。IPv6 NetStream可以与访问控制列表（Access Control List，ACL）和服务质量（Quality of Service，QoS）配合使用，NetStream只统计符合ACL和QoS筛选出的特定报文。可以让针对用户关注的数据进行分析，并且提高了统计多样性。

NetFlow/Netstream本身的流量数据内容很全面，能够单独提供数据流作为流量分析源数据，而且本身不需要其他设备的支持，国内外的一些大型网络运营商已经开始使用，并取得较好的效果。但该功能对网络设备的资源存在一定的消耗，对网络设备性能要求较高。

3）基于IPFIX的流量分析技术

IPFIX的目标是对网络流量测量提供一种通用的规范，这种通用的规范能够在不同的网络设备上使用。

3. 流量分析部署方案

网络流量分析系统的效率不仅要依赖于流量分析技术，而且依赖于系统的安装部署框架。可以根据需求选择合适的部署安装方案。根据网络拓扑结构，一般有集中式和分布式两种网络流量分析部署方案。

集中式网络流量分析部署方案是指将流量分析系统安装于一台服务器上，流量分析的整个过程包括流量获取、分析、存储、展示等操作在同一台服务器上完成。

分布式网络流量分析部署方案是指将流量采集分析服务模块安装在网络多个服务器上，这些服务器将处理结果发送给主服务器或者将结果存储在其自带的存储系统里，主服务器查询时从这些存储系统里获取数据。

集中式流量分析部署方案结构简单，将流量分析系统部署在主要节点上就可以对网络进行监控，但无法满足大规模、复杂的网络结构的需求，适用于线形或者星状网络拓扑结构的网络。

分布式流量分析部署方案可以处理复杂网络结构的流量分析问题，分析结果的汇总及发送等操作也使得分布式的方案速度比集中式方案的要慢，适用于网络拓扑结构复杂的网络。

7.3 通信网性能分析与探测技术

7.3.1 网络性能保障概述

通信网中性能管理的被管对象包括网络中的线路和通信设备。被管对象属性包括流量、时延、丢包率、CPU利用率、温度、内存余量等性能指标。性能指标的测量值是体现

网络设备运行和通信情况的基本信息，是综合网络管理系统中性能管理模块能够工作的基本元素。通过对性能网络设备性能指标测量值的分析和统计，能直观呈现某个网络设备以及端口历史的和当前的工作状况，对网络的评估以及优化具有很重要的意义。

不同通信技术的不同性能指标具有不同的取值范围，比如CPU利用率的范围通常是[0，1]。性能门限作为这个取值范围的子集，描述的是性能指标测量值的合理性，也就是说性能门限确定了当前设备运行的正常情况。当设备的性能指标测量值越过了性能门限的设置值时，说明设备正处于不健康的运行状态中，可能会发生不可预料的情况，会触发相应的性能越限告警。

通常，性能门限值的设定通过设备的历史运行趋势来进行手动设置，需要人为地观察历史性能趋势曲线，选取合理的性能门限值。目前，已经有许多学者对性能门限的自动设置做了研究，这些研究使用一定方法，根据设备的历史性能数据动态地设置性能门限。结合当前项目试点所选取的组网技术，大体来看，作为广泛使用的有线光纤通信技术，EPON以太网具有类似的性能指标，可以从功能上分为两类：与设备运行相关的设备状态性能指标和与网络通信相关的端口状态性能指标。设备状态性能指标主要指能体现设备基本运行性能的一系列测量值，通常包括CPU使用率、内存使用率等；端口状态性能指标主要指能体现设备数据传输性能的一系列测量值，通常包括发送字节数、接收字节数等。其中设备运行相关性能指标统计和端口状态性能指标统计分别如表7-3、表7-4所示。

表7-3 设备运行相关性能指标统计

项　目	单　位	描　述
CPU使用率		表示设备的CPU使用情况
内存使用率		表示设备内存使用情况
内存大小	MB	表示设备的总内存大小
设备响应时间	ms	表示设备的响应时间

表7-4 端口状态性能指标统计

项　目	单　位	描　述
发送速率	kbps	表示当前端口的发送速率
接收速率	kbps	表示当前端口的接收速率
发送字节数	B	端口总的发送字节数
接收字节数	B	端口总的接收字节数
发送错误包数	个	端口发送的错误包总数
接收错误包数	个	端口接受的错误包总数
发送带宽使用率		端口的发送带宽使用率
接收带宽使用率		端口的接收带宽使用率

1） EPON性能指标

EPON采集适配器主要采集OLT设备和ONU设备的性能信息，主要包括OLT设备运行性能、OLT端口状态、ONU端口状态、OLT光模块和ONU光模块几个方面。其中OLT设备运行性能的主要指标同表7-3中列举的设备运行性能指标类似，OLT端口状态和ONU端口

状态的主要性能指标如表7-4所示，OLT光模块和ONU光模块的主要性能指标相同，如表7-5所示。

表7-5　EPON光模块主要性能指标量

项　　目	单　　位	描　　述
发射光功率	dBm	表示当前设备的CPU使用情况
发射光功率	dBm	表示当前设备内存使用情况
温度	℃	光模块的温度
电压	V	光模块的电压

2）工业以太网性能指标

在配用电通信网中，工业以太网作为一种有线光纤通信技术，其采集适配器采集的性能指标主要包括交换机设备指标和端口状态两方面，其性能指标量和OLT相关的性能指标量类似，主要包括设备运行相关性能指标和端口状态相关性能指标，如表7-5所示。

3） PLC和WiMax性能指标

PLC和WiMax由于其通信技术的特性，具有与其通信技术相关的、独特的性能指标。PLC系统与通信性能相关的性能指标主要从通道参数、通道状态和通道质量三个方面考虑，其中与通道参数相关的主要包括上行发送频点、下行发送频点、接收频点、载波机地址和波特率等；与通道状态相关的有发送字节数、接收字节数、信号强度、噪音强度等；与通道质量相关的主要有上行信号强度、下行信号强度、上行噪音强度和下行噪音强度等。

WiMax作为一种无线宽带系统，其性能指标量具有典型的无线网特色，主要有QoS性能测量、流量性能测量、吞吐量性能测量、基站性能测量等。

EPON、工业以太网等有线光纤通信技术在配用电通信网中被广泛应用，并且针对性能采集，已经有了成熟的采集适配器；而PLC和包括WiMax在内的电力无线宽带通信系统作为配用电通信中辅助的通信技术，具有典型的通信特色和性能指标量，尤其并不包含端口状态相关的性能指标。

7.3.2　性能评价体系

1. 指标选取原则

配电网通信系统的性能优劣，主要取决于通信系统运行的具体状况，因此需要认识通信系统运行状态的主要参数，对状态参数进行合理筛选，确定最终的评价指标。评价指标的选取需遵循以下原则：

① 系统性原则：指标的选取应能够反映系统性能的整体状况，建立一个目标明确、结构清晰的多因素、多层次、相互独立的综合指标体系，微观与宏观分析相结合，定量分

析与定性分析相结合。

② 通用性原则：由于各个地区配电网运行及其通信设备的差异性，在建立评估指标体系的时候应尽量考虑到其通用性和适用性，尽可能满足不同地区配电网通信性能评价的要求。

③ 操作性原则：在建立指标体系时，所需指标数据原则上应从现有统计指标中产生。少量需重新统计的指标应是确定的且易于采集的。指标的计算和评价方法的选取应易于操作实施。

④ 独立性原则：指标之间应尽量减少交叉，防止相互包含，要具有相对独立性，每个指标应相对独立地反映评估对象的一个方面，评估指标应可以独立地评估系统中的某项具体内容。

2. 指标体系构建

指标体系的构建可参考一般通信系统的主要性能指标，同时考虑配电网通信系统在信息传输技术和传输质量方面的特殊性，从技术性、可靠性、安全性和扩展性四个方面评价配电网通信系统的综合性能。

1）技术性

技术性是指配电网自动化系统选择通信方式时必须满足的一些硬性要求，例如在传输故障信号时对连通时间的要求必须高效，否则无法达到实施配电网自动化的目的。配电网通信系统的技术性可以从以下四个方面进行评价：ⓐ配电终端的平均传输速率（T1），其值（bps）可以通过厂家提供的理论值得到，也可以通过测量每个配电终端的传输速率，计算覆盖区域配电终端传输速率的平均值得到；ⓑ建立通信连接的平均时间（T2），其值（m/s）主要通过设备测试获取；ⓒ通信系统带宽（T3），其值（Mbps）主要根据厂家提供的设备参数获取；ⓓ通信系统终端覆盖率（T4），其值为每个基站对配电通信终端站点的覆盖程度，根据配电网架构情况获取该数据。

2）可靠性

实施配电网通信的出发点是提高配电网自动化水平，提升配电网的供电质量。一个优良的配电网自动化系统要求通信网络能够进行准确可靠的信息传输。配电网通信系统的可靠性主要用以下四个指标衡量：ⓐ通道可靠率（R1），其值为在统计期间内，对调度点有效服务总小时与统计期间小时数的比值；ⓑ通道平均中断次数（R2），其值为调度点通道在统计期间内的平均中断次数；ⓒ误码率（R3），其值为传输中的误码与所传输的总码数的比值，衡量通信系统在规定时间内数据传输的精确性。

3）安全性

电力通信网络的安全性是保证通信系统进行有效信息传输的必要条件，为了保证配电网自动化系统中通信网络的安全、有效运行，有必要对通信系统进行安全风险分析。配电网通信系统的安全性主要从以下几方面进行评价：ⓐ通信站达标率（S1），其值为

通过对通信站的统计数据获取，一般选取2～3年内通信站达标情况的平均值；ⓑ通信系统抗干扰能力（S2）指通信系统抵抗外界电磁波等信号干扰的能力，其值通过专家打分获取，数值越大代表网络抗干扰能力越强；ⓒ网络自愈能力（S3）指配电网通信系统某一节点故障后系统整体自动恢复正常状态的能力，通过专家打分获取，数值越大代表网络自愈能力越强。

4）扩展性

由于经济的快速发展，配电网本身也在不断改造扩容，因此配电网通信系统一方面要满足未来新增设备接入的要求，另一方面需要考虑适应技术的发展，便于采用性价比更高的新技术。配电网通信系统的扩展性主要指通信系统的标准化程度和通信系统的扩展度。

标准化程度主要包括通信设备的标准化程度（E1）、通信技术的标准化程度（E2）和通信协议的标准化程度（E3），各项指标通过专家打分获取。可扩展程度（E4）主要指现行通信系统能否进行功能扩充和等级提升，能否满足未来通信要求，通过专家打分获取，数值越大代表可扩充性越好。在实际项目分析中，根据配电网终期规模考虑通信方式的可扩充性指标。

通过对配电网通信系统技术性、可靠性、安全性和扩展性方面的分析，构建配电网通信系统综合性能评价指标体系，如表7-6所示。

表7-6 配电网通信系统综合性能评价指标体系

一级指标	二级指标	三级指标
通信系统综合性能	技术性（T）	终端平均传输速率（T1）
		通信平均连接时间（T2）
		通信系统带宽（T3）
		通信系统终端覆盖率（T4）
	可靠性（R）	通道可靠率（R1）
		通道平均中断次数（R2）
		误码率（R3）
	安全性（S）	通信站达标率（S1）
		通信系统抗干扰能力（S2）
		网络自愈能力（S3）
	扩展性（E）	设备标准化（E1）
		技术标准化（E2）
		协议标准化（E3）
		可扩展程度（E4）

7.3.3 网络性能指标

本节从网络性能和业务性能层面对全网性能进行分析，如图7-1所示。

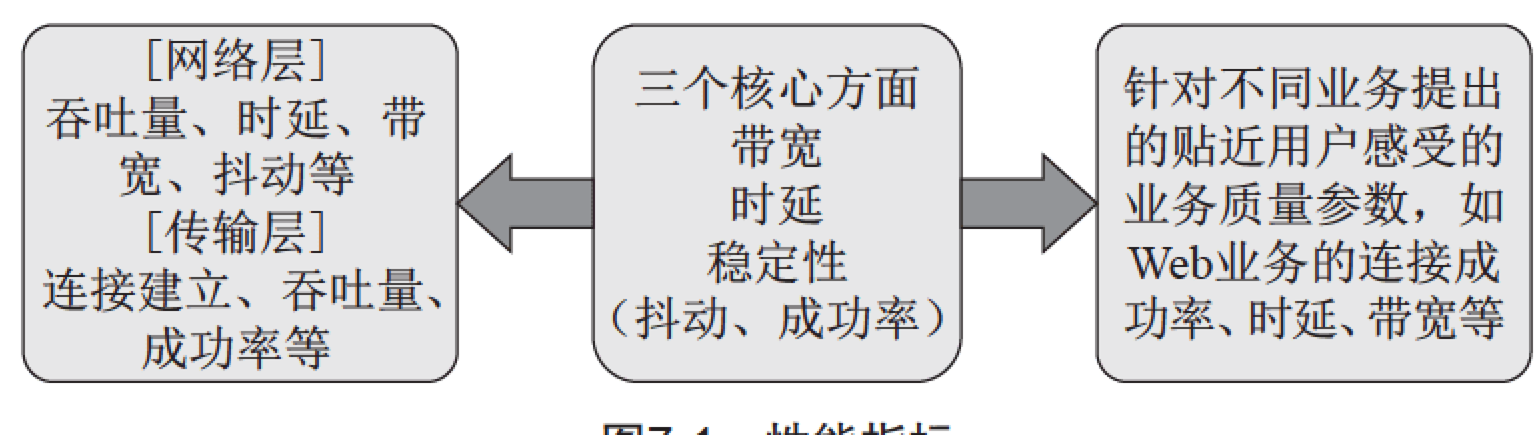


图7-1　性能指标

网络层性能指标包括最小传输时延、最大传输时延、平均传输时延、时延抖动、丢包率、传输速率；时延、时延抖动具体为传输、传播、排队、处理时延；带宽、瓶颈带宽具体为选择不同大小数据包进行测试对比结果的影响；丢包率。

传输层性能指标包括连接建立延时、连接建立成功率、吞吐量、链路通断状态、链路时延、链路时延抖动、链路丢包率、链路可用带宽等。

网络层更关注数据传输的丢包率以及数据的实时性问题，故通过Ping测试和Trace测试测量网络的丢包率、时延、跳数等信息。

网络层的实时性能监控指标如表7-7所示。

表7-7　网络性能评价指标

层　次	分　类	指 标 名 称	指 标 定 义	单　位
网络层	Ping测试	Ping丢包率	（发送包数−接收包数）/发送包数×100	
		Ping时延	成功发送（ICMP echo request）到成功接收（ICMP echo reply）经过的时长	ms
		TTL	ICMP Echo reply记录的TTL	
	Trace测试	跳点数	跟踪记录从源到目标的路由节点数	
		跳点IP	每一个路由节点的IP	
		时延	从源到路由节点的时延	ms

7.3.4　网络性能探测技术

网络性能探测主要通过模拟用户发出的ICMP echo请求，统计分析回应的数据包，计算相应质量指标。主要拨测内容为丢包率和时延，具体流程如下。

1. 网络层丢包率测试

如图7-2所示，探针拨测代理根据拨测任务，按照固定间隔时间向服务器发送N次测试，每次测试发送M个ICMP echo请求数据包，并根据接收到的ICMP echo response响应数据包W个数据包进行丢包率的统计。

该参数的计算公式为：

$$平均网络层丢包率=\frac{(W_1+W_2+\cdots+W_n)-(M_1+M_2+\cdots+M_n)}{n}\times 100\%$$

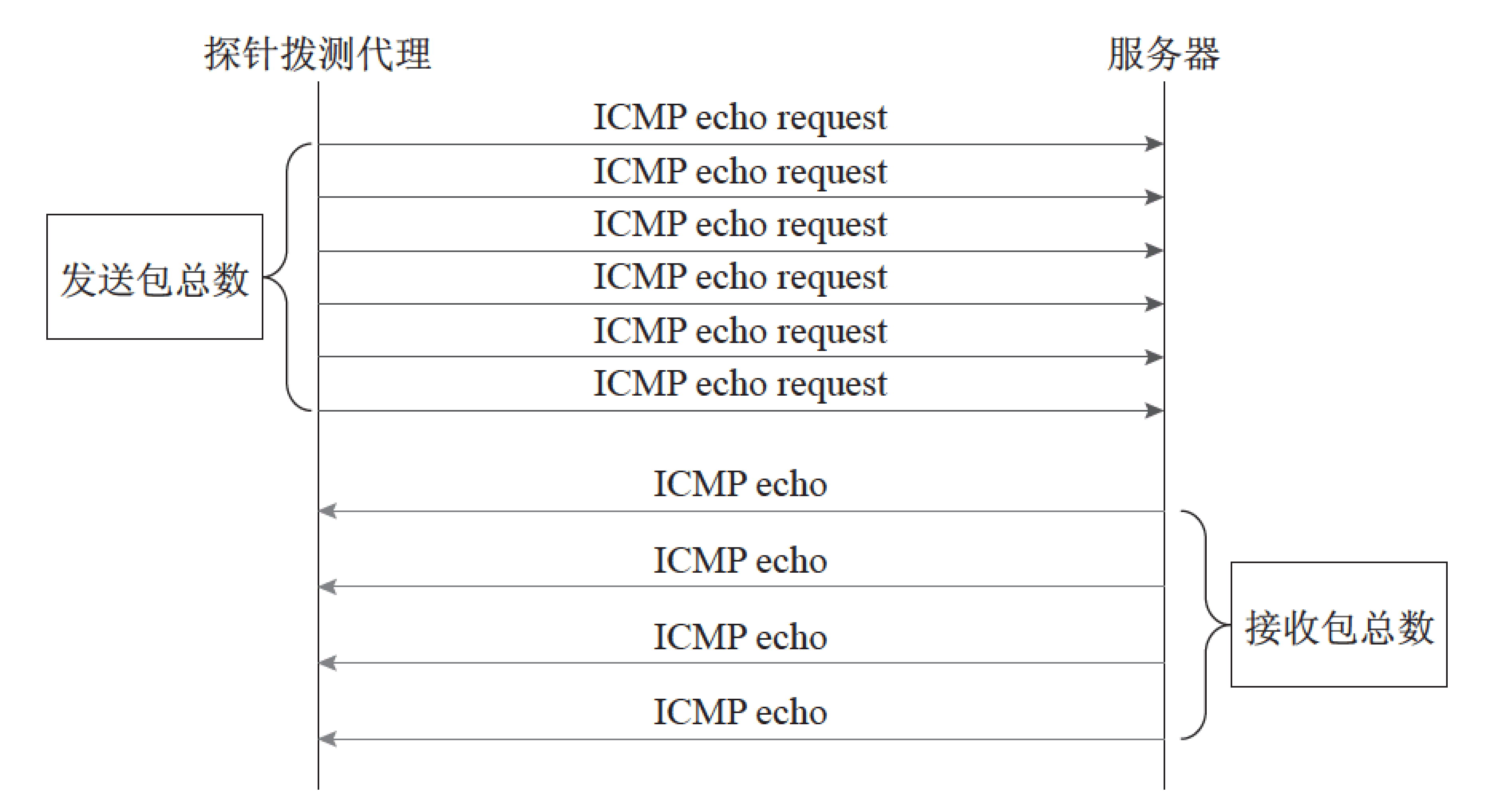


图7-2　网络层丢包率测试示意图

2. 网络层时延测试

如图7-3所示，探针拨测代理根据拨测任务，按照固定间隔时间向服务器发送N次测试，每次测试发送ICMP echo请求数据包并记录起始时间S，只针对接收到ICMP echo响应的往返数据包记录接收时间E，ICMP echo请求没有回应的数据包不计算时延。

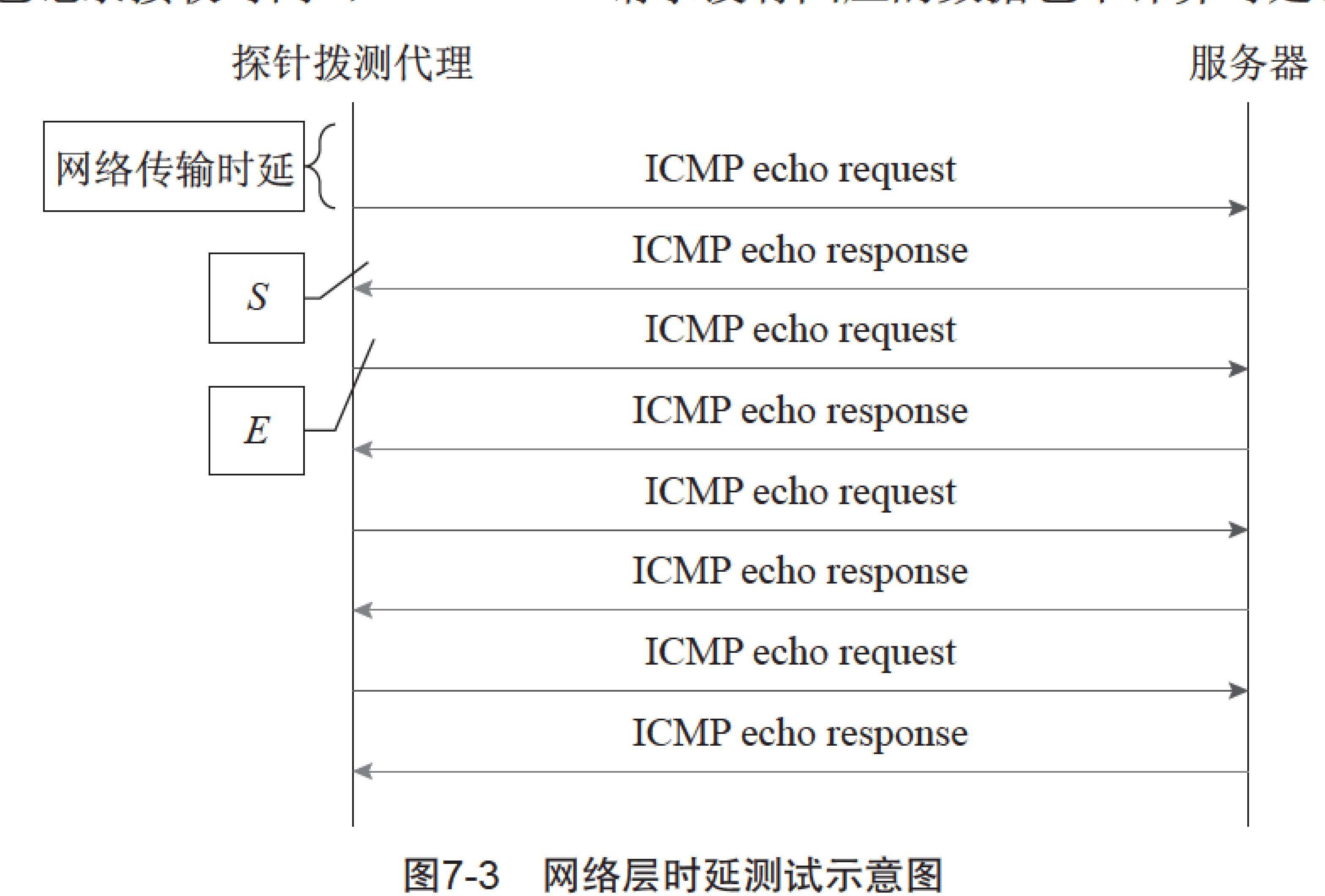


图7-3　网络层时延测试示意图

计算公式如下：

最大网络传输时延$=\max\{(E_1-S_1)\text{or}(E_2-S_2)\text{or}(E_n-S_n)\}$

最小网络传输时延$=\min\{(E_1-S_1)\text{or}(E_2-S_2)\text{or}(E_n-S_n)\}$

平均网络传输时延$=\dfrac{(E_1+E_2+\cdots+E_n)-(S_1+S_2+\cdots+S_n)}{n}\times100\%$

7.4 基于探针的故障定位技术方案

7.4.1 故障检测的探测选择技术

1. 故障检测的探针选择概述

故障检测的目的是检测网络中是否存在故障。只需所选的测试路径满足覆盖网络中的所有节点，由探测站点向其他所有节点产生的探测路径便形成了所有可用探测集合。在故障检测阶段，需要在可用探测集合中选择出一部分探测路径作为故障检测集合。故障检测集合的选取需满足以下条件：

① 所选的测试路径覆盖网络中的所有节点。

② 测试路径尽量少。

故障检测的探测选择问题是一个二分覆盖问题，已被证明是NP完全问题，目前常用的基本方法是基于贪心算法的近似算法。本书通过对贪心算法进行改进来解决故障检测阶段的探测选择问题。

对于故障检测阶段的探测选择的评估指标有：

① 节点覆盖率。

② 探测路径个数。

2. 故障检测的探针选择模型

首先，用探测依赖矩阵可以解决故障检测的选择问题。探测依赖矩阵表明了网络节点与探测之间的依赖关系。对于一个拓扑结构已知的网络来说，已知节点集合N，可用探测集合T。探测依赖矩阵D是一个$n \cdot t$的矩阵，其中$n=|N|$，是网络中节点的个数，$t=|T|$，是可用探测集合中探测的个数。如果探测T_i经过节点N_j，则$\boldsymbol{D}(i, j)=1$；反之，$\boldsymbol{D}(i, j)=0$。

建立探测依赖模型之后，故障检测阶段的探测选择就转化成了选取尽量少的行数包含所有的列，即：

$$T^* = \arg\min\{|T_s| \mid \forall n \in T_s\} \quad (7\text{-}1)$$

其中T^*是我们选取的故障检查集合，T_s是满足包含所有节点的探测集合，$|T_s|$是该探测集合中的探测个数。

3. 故障检测的探针选择方法

1）方法思路

目前常见的贪心策略求解思路有两种：

① 贪心增加算法：设初始化探测集合为空，不断选取能够覆盖最多的尚未被覆盖节点的探测，直到所有节点都被覆盖。

② 贪心减少算法：将所有探测的全集设为初始化探测集合，不断尝试删除某个探测，只需判定该探测的删除不会导致某些节点不被覆盖，直到探测集合中没有这样的冗余探测为止。

虽然这两种算法选择出的探测集合都能覆盖到网络中的所有节点，但是选择出来的探测集合并不一定是最小的探测集合。相对于贪心增加算法，贪心减少算法存在着较多的不确定性，我们可以将贪心增加算法做一定的改进，以提高算法的性能。

改进算法在开始选择时，不是首先选择覆盖最多节点的探测，而是先挑选出被最少探测覆盖的节点，再从能覆盖到该节点的探测中选出覆盖最多节点的探测。在探测依赖矩阵中，每一列向量对应一个节点被探测经过的状态，计算每个节点对应的列向量的权值，可以得出经过每个节点的探测数。在找出被最少探测经过的节点后，可以通过计算经过它的所有探测的行向量的权值，并进行降序排列，来找出覆盖最多尚未被覆盖节点的探测。如此循环，直到所有的节点均被覆盖。

2）算法流程

步骤1　初始化，设探测集合为空。

步骤2　选取被最少探测覆盖的节点N_j，即探测依赖矩阵中列向量的权值最小的列对应的节点。

步骤3　从能覆盖到节点N_j的探测中选出覆盖最多节点的探测T_i，然后删除该探测所覆盖的所有节点，即探测依赖矩阵中能覆盖节点N_j的行向量的权值最大的列。然后删除该列覆盖的节点所对应的列。

步骤4　重复步骤2、步骤3，直到所有的节点被覆盖。

图7-4所示为算法流程示意图。

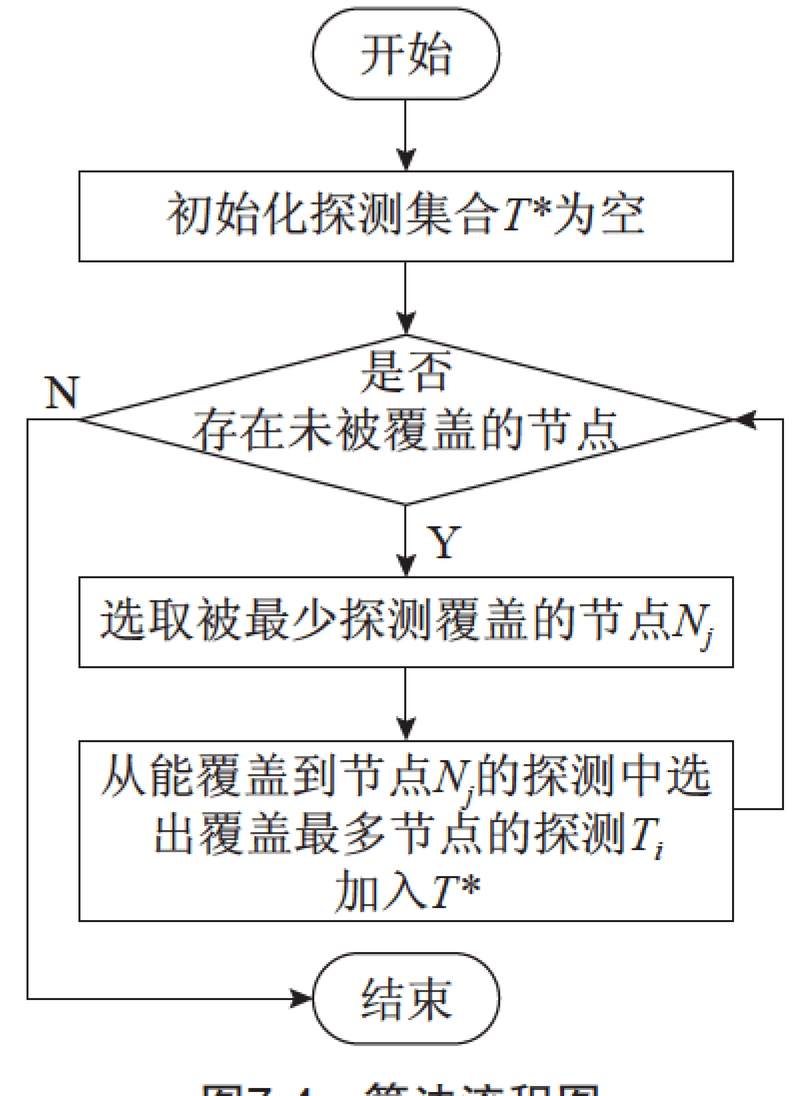


图7-4　算法流程图

7.4.2　故障定位的探测选择技术

1. 故障定位的探测选择概述

当前一阶段故障检测完成后，我们会对探测结果进行分析，如检测到故障的存在，那么就会进行故障定位阶段的探测选择，目的是定位故障的根源。为了达到这个目的，需要发送合适的探测来获取更多的信息。

首先，我们先对故障检测的探测结果进行分析。若探测成功，就认为成功探测经过的所有节点均为正常节点，并将这些节点加入正常节点集合N_{nn}（Normal Node），若有节点之前被判定为可疑节点，将其从可疑节点集合中删除；若探测失败，则失败探测路径上所有之前未被判定为正常节点的节点均为可疑节点，并加入可疑节点集合N_{sn}（Suspicious Node）；若一条失败探测所经过的所有节点中，仅有一个节点为可疑节点，其他节点都被某些成功探测经过，那么该可疑节点即为故障节点，并被加入故障节点集合N_{fn}（Fault Node）。

然后，通过对故障检测阶段探测返回结果的分析，可以得出正常节点集合、可疑节点集合以及故障节点集合。而可疑节点集合作为状态不确定的节点集合，将成为故障定位阶段的探测的目标。目前故障定位阶段的探测选择方法有两大类：预先选择探测方式和交互式选择探测方式。预先选择探测方式一次性选择出所有故障定位探测集合，发送到网络中并接收探测结果，这种方式对网络施加固定的负荷，虽然计算过程比较简单，但是对所有的探测执行如此计算是极其低效的；交互式的探测方式是每次根据上一次探测的探测结果自适应地选择下一个探测，这样可以有效减少所需执行探测的数量，从而得到更好的时效性和更低的额外网络负载，但计算过程往往异常复杂。本书选择交互式的探测思路来设计算法。

故障定位阶段的探测选择要求选择一个新的探测，该探测将要使可疑节点集合中的节点数量尽量减少。这样选择的探测次数才会更少，能够带来更少的额外网络负担。

对于故障定位阶段的探测选择的评估指标有：

① 探测次数。

② 判定故障节点的正确率。

2. 故障定位的探测选择模型

故障定位阶段的探测选择的建模也是探测依赖矩阵，和故障探测阶段的探测选择不同的是，此阶段的探测选择是从备选探测集合（未被作为探测的探测集合，在故障检测阶段表示除了故障检测集合以外的可用探测集合，在故障定位阶段表示除了故障检测集合和之前故障定位探测以外的可用探测集合）里面选取满足使可疑节点数尽量减少的探测。所以

本阶段的探测必须覆盖可疑节点。

对于减少可疑节点有以下两种情况：

① 若只覆盖一个可疑节点的探测测试结果返回失败，则表明该可疑节点为故障节点；

② 若覆盖可疑节点的探测测试结果返回成功，则表明这些可疑节点为正常节点。

需要注意的是对于第2种情况，还要考虑由于把这些可疑节点从可疑节点集合删除，加入正常节点集合之后，之前测试集合中结果返回失败且覆盖多个可疑节点的探测可能现在只含有一个可疑节点了，需要对所有的然后失败的探测集合重新进行情况1的判定。

3. 故障定位的探测选择方法

1）方法思路

故障定位阶段的探测选择有两种基本思路：

① MAX算法：每次选择一个经历N_{sn}中节点最多的探测。若这次探测成功，则将使得N_{sn}中的节点减少很多；反之，不能减少N_{sn}的节点。注意经历N_{sn}中所有节点的探测除外，因为该探测一定返回失败。

② MIN算法：每次选择经历N_{sn}中节点最少（至少为1个）的探测。若这次探测成功，则将使N_{sn}中的节点减少至少1个，若探测失败，且当且仅当它经历一个节点时，我们把该节点从N_{sn}中删除并加入N_{fn}。

一般来说，考虑到网络中出现故障的节点总是少数的，相对来说即使经历N_{sn}中节点较多的探测成功的可能性也高于失败的可能性，选择Max算法会更好一些，但是由于我们在探测站点的选择上只使用3个节点，会导致很多可疑节点是故障节点的后续节点，即这些可疑节点会伴随着故障节点一起出现，导致经历N_{sn}中节点较多的探测失败的可能性大大增加，所以我们选择Min算法。

2）预处理

对于故障检测阶段测试结果分析：

① 把所有节点分别加入N_{nn}、N_{sn}、N_{fn}中。

② 记录所有返回结果失败的测试，把它们放到测试失败集合T_{ft}（Fault Test）中。

③ 将备用探测集合中经历故障节点的探测删除。

3）算法流程

步骤1　若$|N_{sn}|$为空或者备用探测集合中不包含经历可疑节点的探测则退出，否则将备用测试集合中所有经历N_{fn}的探测从备用测试集合中删除，然后转入步骤2。

步骤2　在备用探测集合选择经历N_{sn}中节点最少（至少为1个）的探测T_i，然后转入步骤3。

步骤3　若T_i探测结果返回成功，则将该探测中经历N_{sn}中节点从N_{sn}中删除并加入N_{nn}，然后转入步骤4；若T_i探测结果返回失败，将该探测加入T_{ft}，若在结果返回失败且该探测中

仅有1个可疑节点，则将该可疑节点从N_{sn}中删除并加入N_{fn}中，然后转入步骤1。

步骤4　历遍T_{ft}，将其中满足有且仅有1个可疑节点的探测中的可疑节点从N_{sn}中删除并加入N_{fn}中，然后转入步骤1。

图7-5所示为算法的流程图。

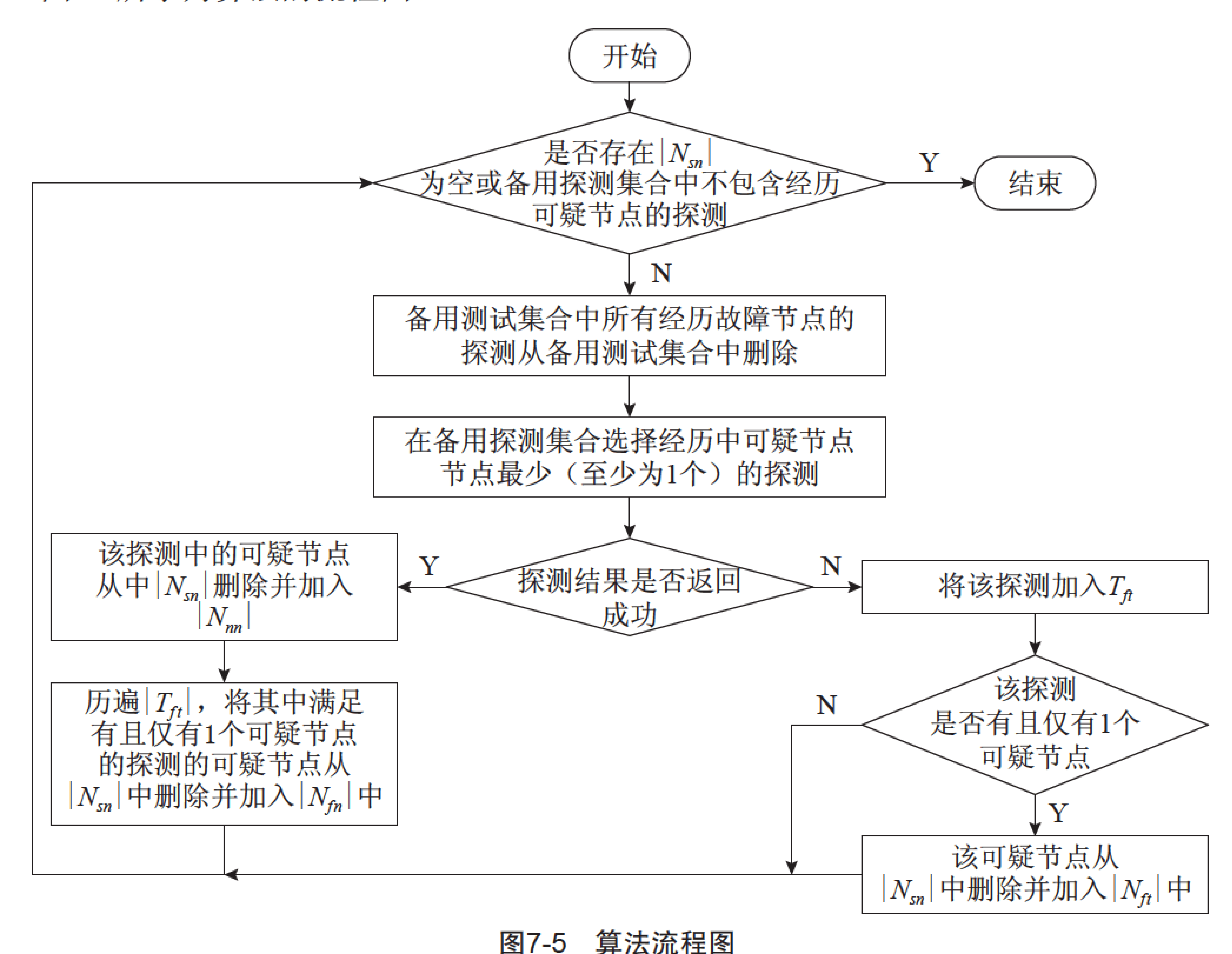


图7-5　算法流程图

7.5　网络性能保障机制研究

1. 研究背景

网络虚拟化技术最先被应用于互联网，为了提高电力通信网络的灵活性与资源的利用率，虚拟化技术也逐渐被应用到电力通信网络中。将电力通信网络中服务层的业务请求映射到基础设施层，每个请求在基础设施层只会被分配一条路径。一旦底层网络出现故障就无法正常为服务层提供所需的资源，在对网络可靠性要求较高的电力通信网络中这是个急需解决的问题。在出现故障的情况下；将服务层的业务请求有效地映射到基础设施层，既能提高电力通信网络的可靠性又能保证网络的负载均衡，变得尤为重要。

2. 问题分析

电力通信网络的业务有需求响应业务、继电保护业务、调度自动化、电网运行维护检修和生产管理等多种。在电力通信网的基础设施层有不同种类的通信设备与介质，这里只考虑它们的共有属性，即通信设备的计算能力和通信介质的带宽。在故障方面，本书只考虑单点故障。

相关的参数变量如表7-8所示。

表7-8　相关参数变量

参 数 变 量	表 示 意 义
$\boldsymbol{G}^V\left(N^V,E^V\right)$	以虚拟网络提供层的节点为行，链路为列组成的无向图矩阵
$\boldsymbol{G}^S\left(N^S,E^S\right)$	以虚拟网络的节点为行，链路为列组成的无向图矩阵
$R_N(i)\ ,i\in N^V$	虚拟网络提供层节点的剩余计算能力
$R_{NMax}(i)\ ,i\in N^V$	虚拟网络提供层节点的最大计算能力
$R_E(i)\ ,i\in E^V$	虚拟网络提供层链路的剩余带宽
$R_{EMax}(i)\ ,i\in E^V$	虚拟网络提供层链路的最大带宽
$c(i),i\in N^S$	服务层节点的计算能力需求
$b(i)\ ,i\in E^S$	服务层链路的带宽需求
α	虚拟网络提供层主链路的百分比
β	虚拟网络提供层辅链路的百分比，$\beta=1-\alpha$
$\varphi_l(s) l\in E^S,s\in E^V$	路径的指示变量
$Ratio^N(i)\ ,i\in N^V$	虚拟网络提供层节点负载率
$Ratio^E(i)\ ,i\in E^V$	虚拟网络提供层链路负载率
$length(l),l\in E^S$	服务层链路映射到虚拟网络提供层链路的跳数
$\delta(s)\ ,s\in N^V$	虚拟网络提供层链路是否有映射的指示变量
$Var\text{-}Ration(p)$	负载方差
$T(l)$	虚拟链路允许的最大映射跳数

1）网络模型

（1）虚拟网络提供层网络模型：

虚拟网络提供层网络模型使用无向带权图 $\boldsymbol{G}^V=\left(N^V,E^V\right)$ 表示，其中 N^V 表示虚拟网络提供层中节点的集合，E^V 表示虚拟网络提供层中链路的集合，权值是每条链路的剩余带宽。对于每个虚拟网络提供层节点 $n_i^V\in N^V$，它具有以下属性：虚拟网络提供层节点的最大计算能力，记作 $R_{NMax}(i)$；虚拟网络提供层节点的剩余计算能力，记作 $R_N(i)$。对于每条虚拟网络提供层链路 $l_x^V(i,j)\in E^V$，它的总带宽记作 $R_{EMax}(x)$，剩余带宽记做 $R_E(x)$。

（2）虚拟请求网络模型：

虚拟请求网络模型也使用无向带权图$\boldsymbol{G}^{S}=\left(N^{S},E^{S}\right)$表示，其中$N^{S}$表示虚拟请求网络节点中节点的集合，$E^{S}$表示服务层请求中链路的集合，权值是每条链路的请求带宽。在服务层的请求中，对于每一个服务层节点$n_{i}^{S}\in N^{S}$而言，它包含着需要的计算能力$c(i)$，对于每条服务层链路$l_{x}^{S}\in E^{S}$而言，链路所需的带宽大小是$b(x)$。

2）映射模型

（1）S-V layer映射模型：

S-V layer映射模型如图7-6所示。

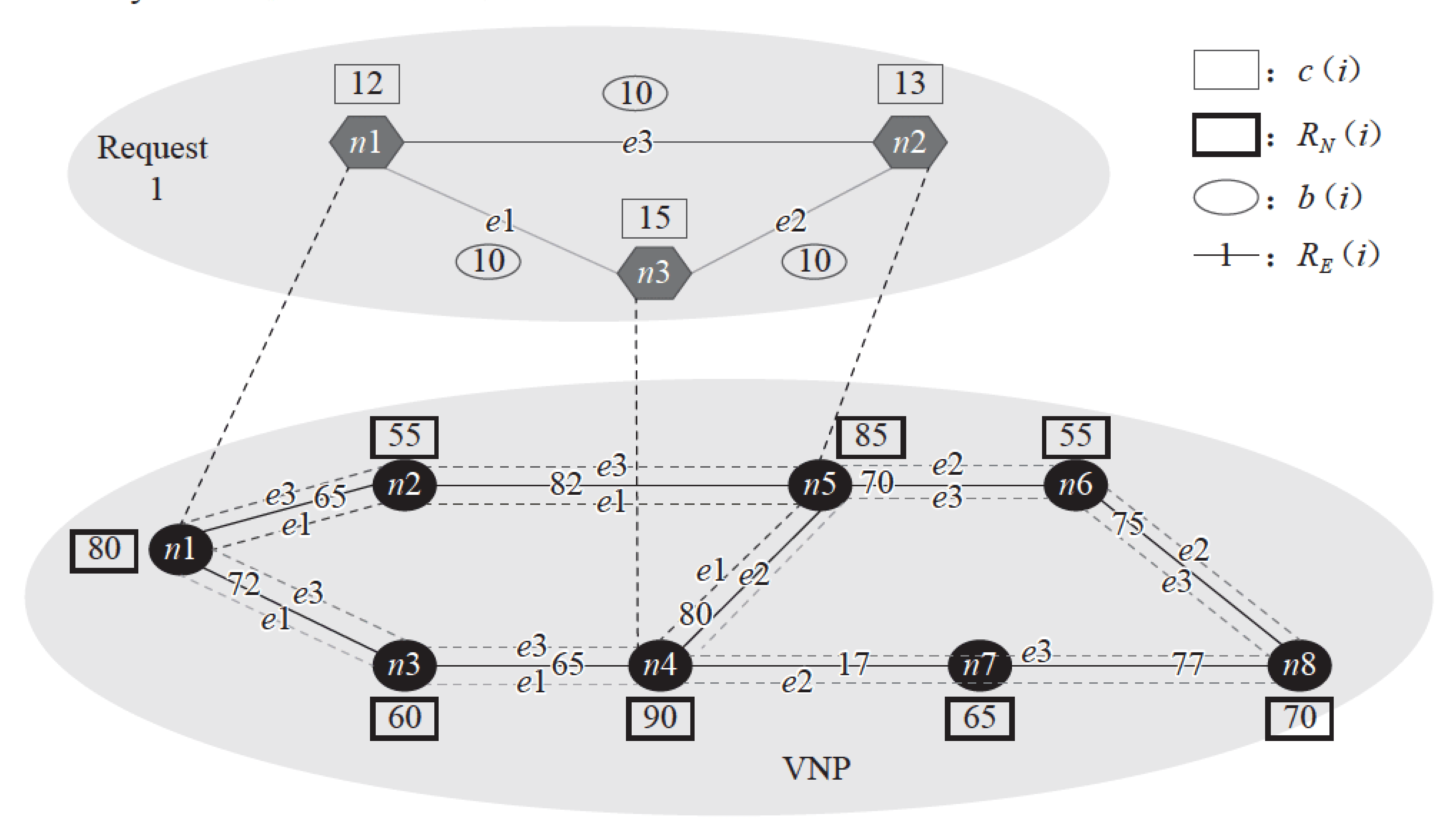


图7-6　S-V layer映射模型

S-V layer映射模型是将服务层的不同业务映射到虚拟网络提供（Vn）层，并形成相互隔离的虚拟子网络。服务层的请求映射到虚拟网络提供层分为两个映射阶段：节点映射阶段和链路映射阶段。

如图7-6所示，图中Request部分的$n1$，$n2$，$n3$节点为服务层的请求节点，VNP部分的$n1$，$n2$，$n3$，…，$n8$节点为虚拟网络提供层的节点，矩形框中的数字为各个节点所需或所能提供的计算能力，椭圆框中的数字为服务层链路所需的带宽，链路上的数字是虚拟网络提供层链路可以提供的带宽。以负载均衡为目标将服务层的节点$n1$，$n2$，$n3$分别映射到虚拟网络提供层的节点$n1$，$n5$，$n4$上。服务层的每条链路在虚拟网络提供层都会有2条链路映射，一条主链路，一条辅链路，如图7-6中服务层链路$e1$，在虚拟网络提供层就有长虚线链路$e1$作为主链路，短虚线链路$e1$作为辅链路，同时主链路与辅链路是不相交的，以保证网络的可靠性。

① 节点映射。

在映射过程中，评价映射是否成功的一个重要指标就是网络的负载均衡。所以我们在节点映射阶段应考虑每个虚拟网络提供层的节点的负载率，记为$Ratio^{N}(i)$，则虚拟网络提供层的节点的负载率可表示为：

$$Ratio^{N}(i)=\frac{R_{N\text{Max}}(i)-R_{N}(i)}{R_{N\text{Max}}(i)} \tag{7-2}$$

节点剩余计算能力的计算公式如下：

$$R_{N}(i)=R_{N}^{'}(i)-c(j) \tag{7-3}$$

$R_{N}^{'}(i)$表示虚拟提供层的节点在为映射此请求节点前所剩余的计算能力。在映射过程中，尽量选取负载率低的节点进行映射。

② 链路映射。

当虚拟请求层的请求节点映射到虚拟网络提供层后，需要将服务层的请求链路映射到虚拟网络提供层。在映射过程中采用了主辅链路共同映射模型，增大了底层网络的负载。所以在映射过程中以负载均衡为目标，计算每条物理链路的负载率，将最小的负载方差作为求解目标。所求的最小目标公式如下：

$$Var\text{-}Ratio(p)=\frac{\sum_{l\in E^{V}}\delta(l)\left(Ratio^{E}(l)-\sum\limits_{l\in E^{V}}Ratio^{E}(l)\right)^{2}}{\sum\limits_{l\in E^{V}}\delta(l)} \tag{7-4}$$

式中，$Var\text{-}Ratio(p)$是虚拟网络提供层中被映射到的链路负载率的方差，这个方差可以用来衡量虚拟网络提供层的负载均衡程度，方差越小负载越均衡，p表示服务请求。若虚拟网络提供层的链路上有虚拟链路映射则$\delta(l)=1$，否则$\delta(l)=0$。$Ratio^{E}(l)$是虚拟网络提供层链路的负载率，其计算公式如下：

$$Ratio^{E}(l)=\frac{R_{E\text{Max}}(l)-R_{E}(l)}{R_{E\text{Max}}(l)} \tag{7-5}$$

虚拟网络提供层的链路剩余带宽计算公式如下：

$$R_{E}(l)=R_{E}^{'}(l)-b(m) \tag{7-6}$$

其中$R_{E}^{'}(l)$表示在未映射请求链路l的链路剩余带宽。

映射过程中的带宽约束如下：

$$C1:\sum_{m\in E^{S}}\varphi_{m}(l)b(m)\leqslant\alpha R_{E}^{'}(l),\ \ \forall l\in E^{V} \tag{7-7}$$

$$C2:\sum_{m\in E^{S}}\varphi_{m}(l)b(m)\leqslant\beta R_{E}^{'}(l),\ \ \forall l\in E^{V} \tag{7-8}$$

上述二式分别是对虚拟网络提供层的主映射链路与辅映射链路的带宽约束，当请求链路m虚拟网络提供层链路l处有主链路映射时，$\varphi_{m}(l)=1$，否则为0。同理，当请求链路m虚拟网络提供层链路l处有辅链路映射时，$\varphi_{m}^{'}(l)=1$，否则为0。同时主链路和辅链路互不相交，其不相交约束公式如下：

$$C3:\varphi_{m}(l)+\varphi_{m}^{'}(l)\leqslant1,\forall m\in E^{S},\forall l\in E^{V} \tag{7-9}$$

$$C4:\varphi_m(l)\in\{0,1\},\forall m\in E^S,\forall l\in E^V \tag{7-10}$$

$$C5:\varphi_m^{'}(l)\in\{0,1\},\forall m\in E^S,\forall l\in E^V \tag{7-11}$$

服务层的业务请求对时延也有要求，在映射过程中需要考虑每个虚拟链路映射到虚拟网络提供层链路后，业务所经过的时延约束：

$$C6:lenrth(l)\leqslant T(l),\forall l\in E^S \tag{7-12}$$

式中，$\text{length}(l)$是请求链路映射到虚拟网络提供层的链路后所经过的跳数，$T(l)$是服务层对业务允许的所经过最大跳数。

因此，S-V layer 映射模型可被描述为：

$$\begin{aligned}&\min:Var\text{ - }Ration(p)\\&s.t.C1,C2,C3,C4,C5,C6\end{aligned} \tag{7-13}$$

（2）V-I layer映射模型

基础设施层两个设备之间的通信传输介质包括光纤、电缆、PLC等，当业务请求从服务层映射到虚拟网络提供层后，在向基础设施层映射时，需要根据业务的QoS要求选取适合的传输通道。

如图7-7所示，假设服务层的服务1已经将资源请求映射到虚拟网络提供层，在虚拟网络提供层上层的虚线表示主链路，中间层的实线表示辅链路，虚拟网络提供层会根据服务层对请求可靠性、时延等的要求，对基础设施层的设备进行选择。基础设施层链路就是服务1根据自身QoS要求而选择的传输链路，从而完成了整个资源映射过程。

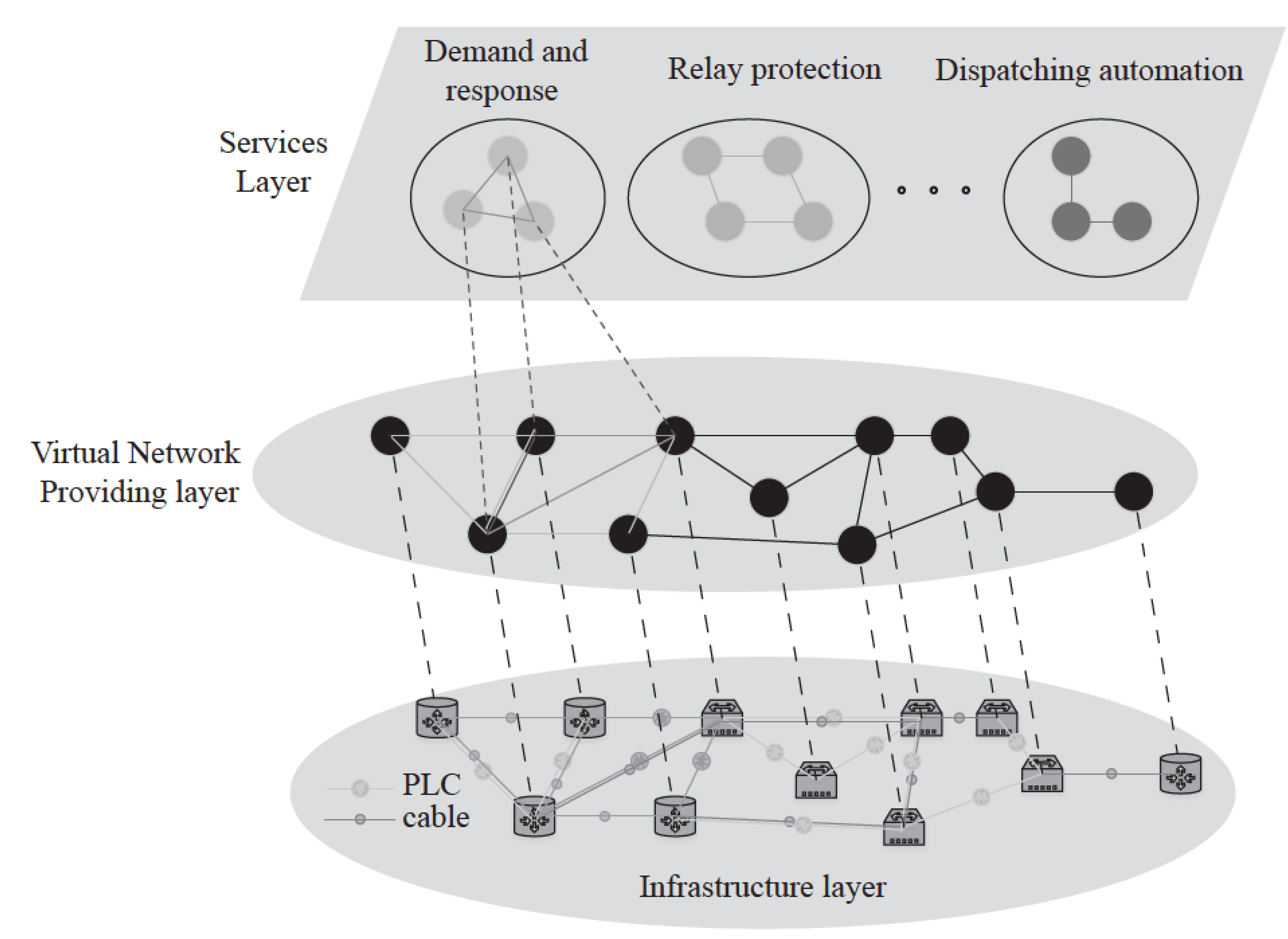


图7-7　V-I layer映射模型

3. 基于负载均衡的虚拟网络映射算法

LFMM分为基于负载均衡的节点映射和基于遗传算法的容错网络链路映射。分别解决在节点映射阶段和链路映射阶段服务层对虚拟网络提供层的网络可靠性的需求问题。

基于负载均衡的节点映射（Load-balancing-based virtual node mapping，LVNM ），在前人的研究中，节点映射阶段一般采用贪婪算法，但是可能会由于网络中个别节点的计算能力很强从而映射了多个请求，造成网络的负载不均衡。为了保证虚拟网络提供层的负载均衡，这里提出基于负载均衡的贪婪映射算法，算法过程为：

① 感知请求节点的计算能力。

② 感知虚拟网络提供层的节点的计算能力，并进行降序排序。

③ 每次都选取服务请求中请求计算能力最大的节点进行映射，在虚拟网络提供层中选出满足计算能力的节点放入一个集合 S 中。

④ 在这个集合 S 中选取负载率最小的节点作为映射节点。

基于遗传算法的容错网络链路映射（Genetic-Algorithm-based fault-tolerant virtual link mapping，GFVLM），由于服务层到虚拟网络提供层的链路映射是NP难题，此处采用遗传算法对 S－V layer 链路映射模型进行求解。

求解的基本流程如下：

编码：采用自然数编码的方式，将0到n之间的自然数进行排序，不同的排序方式表示从起点到终点不同的路径选择。每个染色体就是一个链路映射方案。

初始种群：为了使初始种群均匀地分布在整个解空间，采用部分随机的方式生成初始种群。

适应度函数：在遗传算法当中，染色体的适应度越大，性能就越好。因此需要把模型中的目标函数转化为适应度函数，转化方式如下：

$$f_i = \frac{1}{Z_i}，\ i \in \{1, 2, \cdots, popsize\}$$

式中，f_i表示第i条染色体对应的适应度，Z_i为群体中第i条染色体对应的目标函数值，表示第i条染色体对应的负载方差。

选择算子：采用轮盘赌的方法选择算子。

交叉算子：采用部分匹配交叉算子方法，得到新的链路映射方案。

变异算子：采用翻转变异方式，在一条染色体上随机选取两组变异点，然后通过翻转的方式进行变异。

终止条件：采用达到最大进化迭代次数作为终止条件。

4. 算法仿真

1）参数设置

这里仿真选择了电力通信网络中的需求响应和电力调度自动化两类对网络可靠性要求

较高的业务。虚拟网络提供层的节点计算能力 $R_N(i)$ 和链路带宽 $R_E(j)$ ，服务层的请求节点所需计算能力 $c(i)$ 与链路所需带宽 $b(j)$ 如表7-9所示。将节点负载率 $node_ratio(i)$ 和链路负载率 $link_ratio(j)$ 及其负载方差 $var-Ratio(\pi)$ 作为评价指标对仿真结果进行评价与分析。

仿真采用的数据如表7-9所示。

表7-9　仿真数据表

项目 \ 网络	虚拟网络	请求网络
子网数目	1	2
每张网络的节点数	6	3
每张网络的链路数	15	3

虚拟网络提供层的节点计算能力与链路带宽如表7-10、表7-11所示。

表7-10　虚拟网络提供层节点计算能力表

节　点	计算能力	节　点	计算能力
0	15	3	20
1	21	4	19
2	13	5	12

表7-11　虚拟网络提供层链路带宽表

链　路	带　宽	链　路	带　宽
0	16	8	17
1	10	9	15
2	14	10	13
3	9	11	10
4	10	12	18
5	15	13	12
6	20	14	11
7	19		

需求响应业务的节点计算能力需求与链路、带宽需求如表7-12所示。

表7-12　需求响应业务节点计算能力需求与链路及带宽需求表

节　点	计算能力	链　路	带　宽
0	3	0	3
1	4	1	5
2	5	2	4

电力调度自动化业务的节点计算能力需求与链路、带宽需求如表7-13所示。

表7-13　电力调度自动化业务节点计算能力需求与链路及带宽需求表

节　点	计算能力	链　路	带　宽
0	4	0	3
1	2	1	1
2	6	2	5

2）仿真结果分析

此处仿真分为两个场景，先在小数据的情况下进行网络虚拟化映射，然后扩大数据范围，增加服务层的业务种类与数量，同时增加虚拟网络提供层的节点与链路数量。考察虚拟网络提供层的节点与链路负载率分布是否均衡，并与贪婪算法进行比较，来分析本文所提出的算法是否能够有效均衡网络负载，保障网络的可靠性。

（1）节点映射阶段

基于负载均衡算法进行节点映射所得的映射结果如表7-14所示。

表7-14　节点映射结果表

服务请求	请求节点	虚拟节点
0	0	4
0	1	3
0	2	1
1	0	2
1	1	5
1	2	0

基于负载均衡的贪婪节点映射算法与基本贪婪算法节点映射负载率比较结果如图7-8所示。

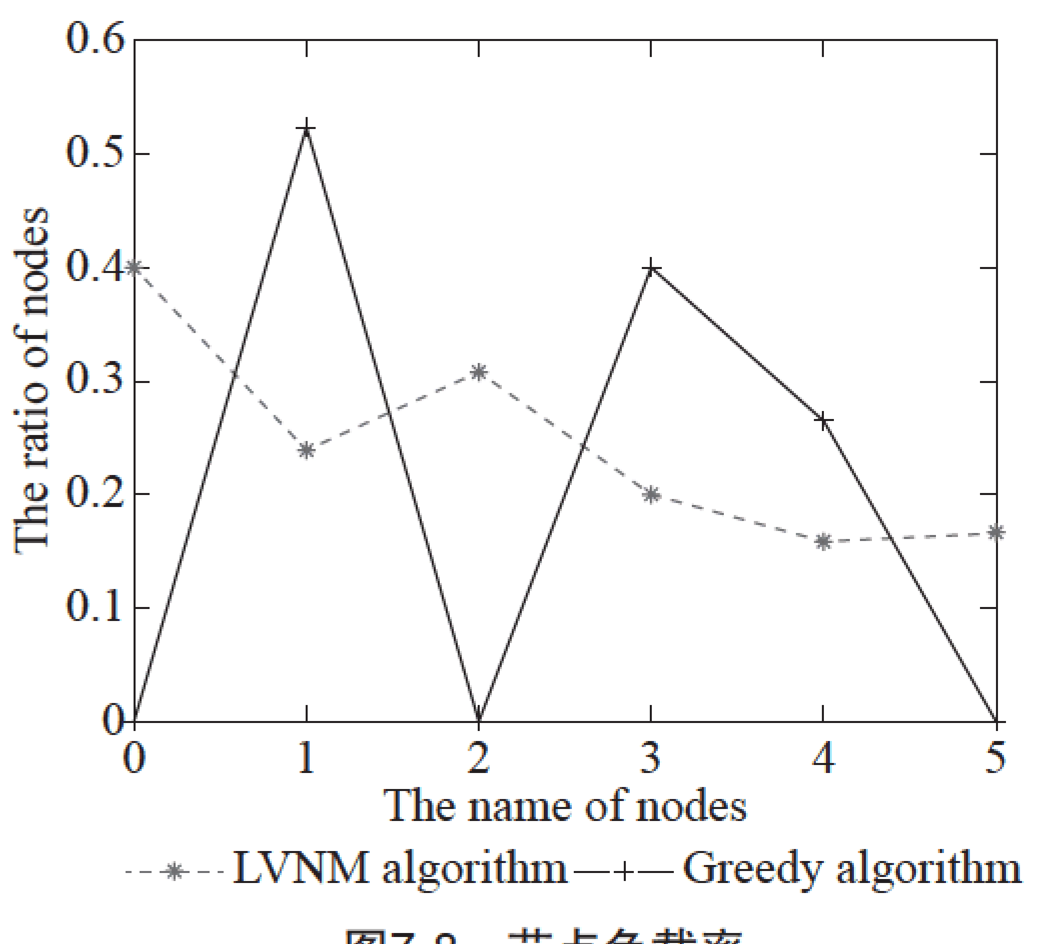


图7-8　节点负载率

如图7-8所示，灰色虚线表示采用基于负载均衡的贪婪算法进行节点映射所得的节点负载率，黑色实线表示使用基本贪婪算法进行节点映射所得的节点负载率。相比于贪婪节点映射算法，采用基于负载均衡的节点映射算法可以使物理节点的负载率更加均衡，提高了网络的可靠性。

（2）链路映射阶段

基于遗传算法主链路映射结果如表7-15所示。

表7-15　遗传算法主链路映射结果表

服务请求	请求链路	虚拟链路
0	0	7→6
0	1	7
0	2	6
1	0	11
1	1	1
1	2	8→5→9→12→3

基于遗传算法辅链路的映射结果如表7-16所示。

表7-16　遗传算法辅链路映射结果表

服务请求	请求链路	虚拟链路
0	0	10→1→0→8→13
0	1	12→6
0	2	2→0
1	0	5→7→14
1	1	9→13→14→3
1	1	4

主链路与辅链路映射完成后物理网络的链路负载情况如图7-9所示。

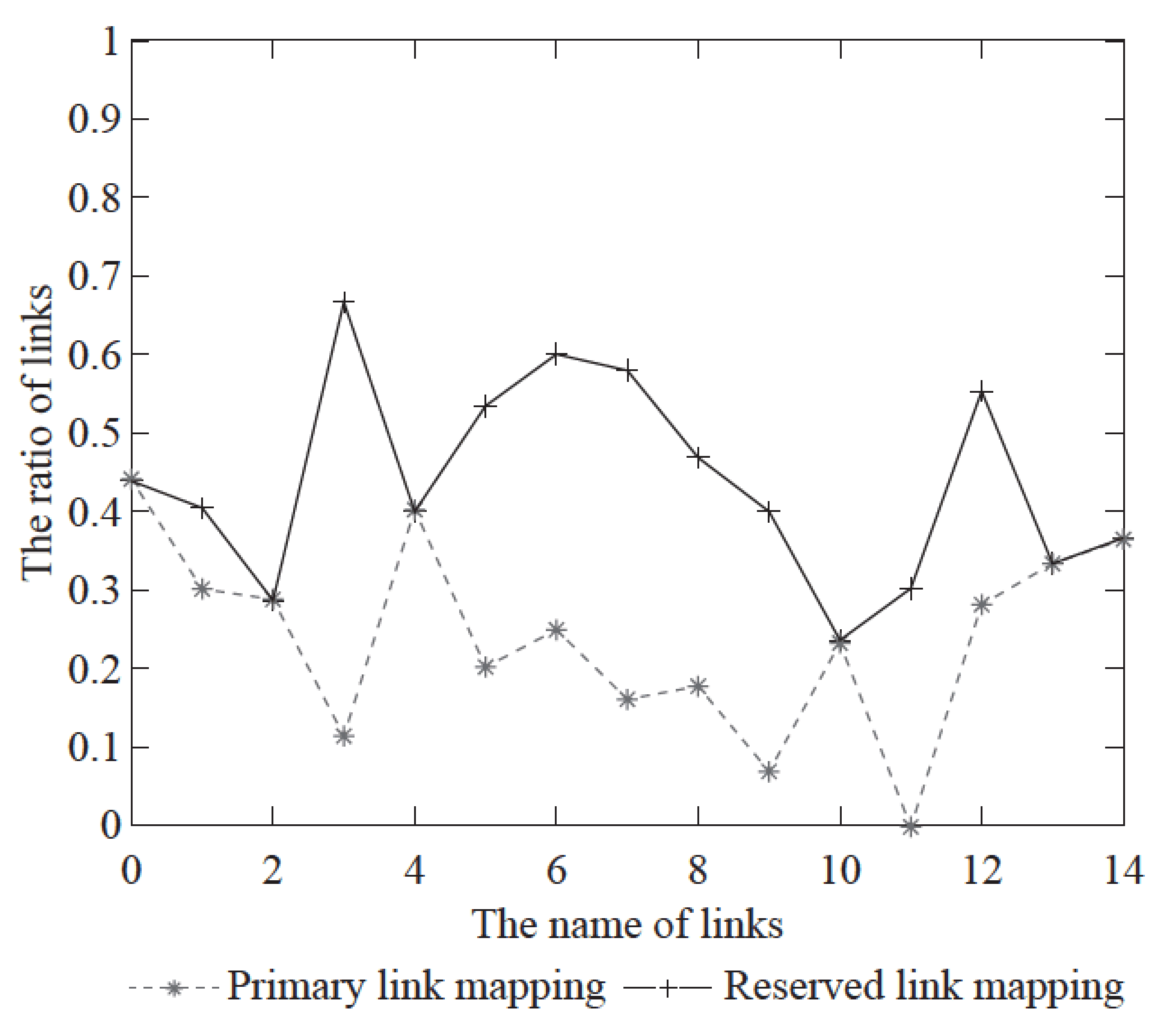


图7-9　物理链路负载率

如图7-9所示，灰色虚线表示利用基于负载均衡的遗传算法进行链路映射，映射完主链路后物理网络的链路负载率，黑色实线表示利用基于负载均衡的遗传算法进行链路映射，辅链路映射完成后物理网络链路的链路负载率。由此可知，随着在虚拟网络提供层网络负载链路的增加，网络整体的负载率呈上升趋势，且整体网络的负载率均衡上升，没有

出现零负载与满负载共存的情况。

在第二个场景中，扩大了数据量以表达实际的电力通信网络中真实的业务数量与种类，同时验证在真实网络环境中本方法的稳定性。底层物理网络的节点数增加到40个，链路数增加到100条。请求网络增加到20张，每张网络仍然有3个虚拟节点与3条虚拟链路。将仿真结果与用贪婪算法所得的结果比较，如图7-10所示。

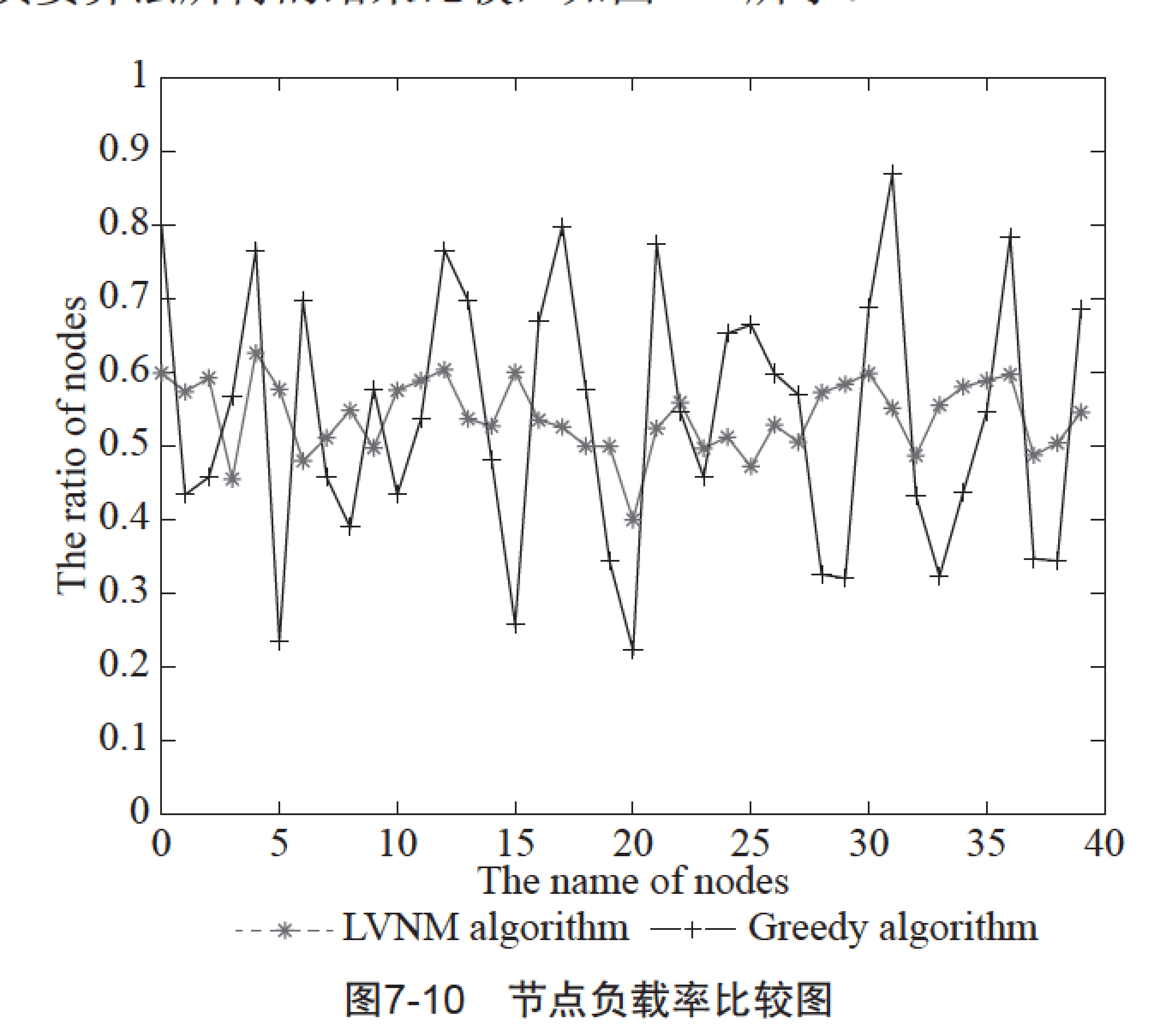


图7-10 节点负载率比较图

图7-10中灰色虚线表示用基于负载均衡的贪婪算法进行节点映射后虚拟网络提供层的节点负载率，黑色实线表示用基本贪婪算法进行节点映射后虚拟网络提供层的节点负载率。将两条虚线进行对比，可知在节点映射阶段，数据量越大，映射的结果越稳定，本例提出的算法有很好的稳定性。

图7-11中*号线表示采用基于负载均衡的遗传算法链路映射方法后虚拟网络提供层的

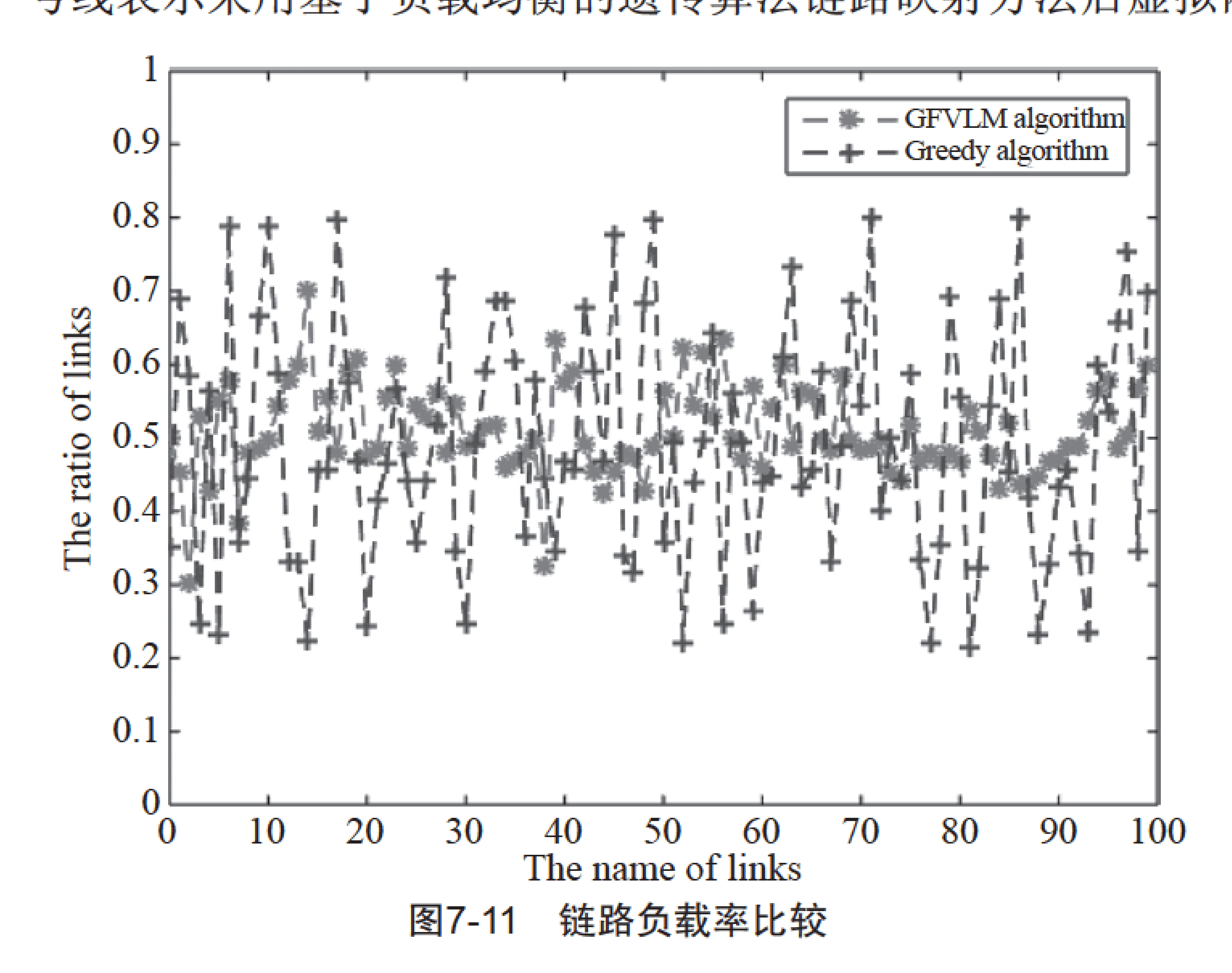


图7-11 链路负载率比较

链路负载率，+号线表示采用基本的贪婪算法进行链路映射后虚拟网络提供层的链路负载率。由此可知，在链路映射阶段，基于负载均衡的遗传算法与贪婪算法在链路映射阶段运行结果更加理想，链路的负载更加均衡，可以很好地保障网络的可靠性，同时随着实验数据的增加，仿真所得的结果也越稳定。

7.6　典型应用环境

7.6.1　典型应用场景

1. 工业以太网故障定位

工业以太网故障检测示意图如图7-12所示。

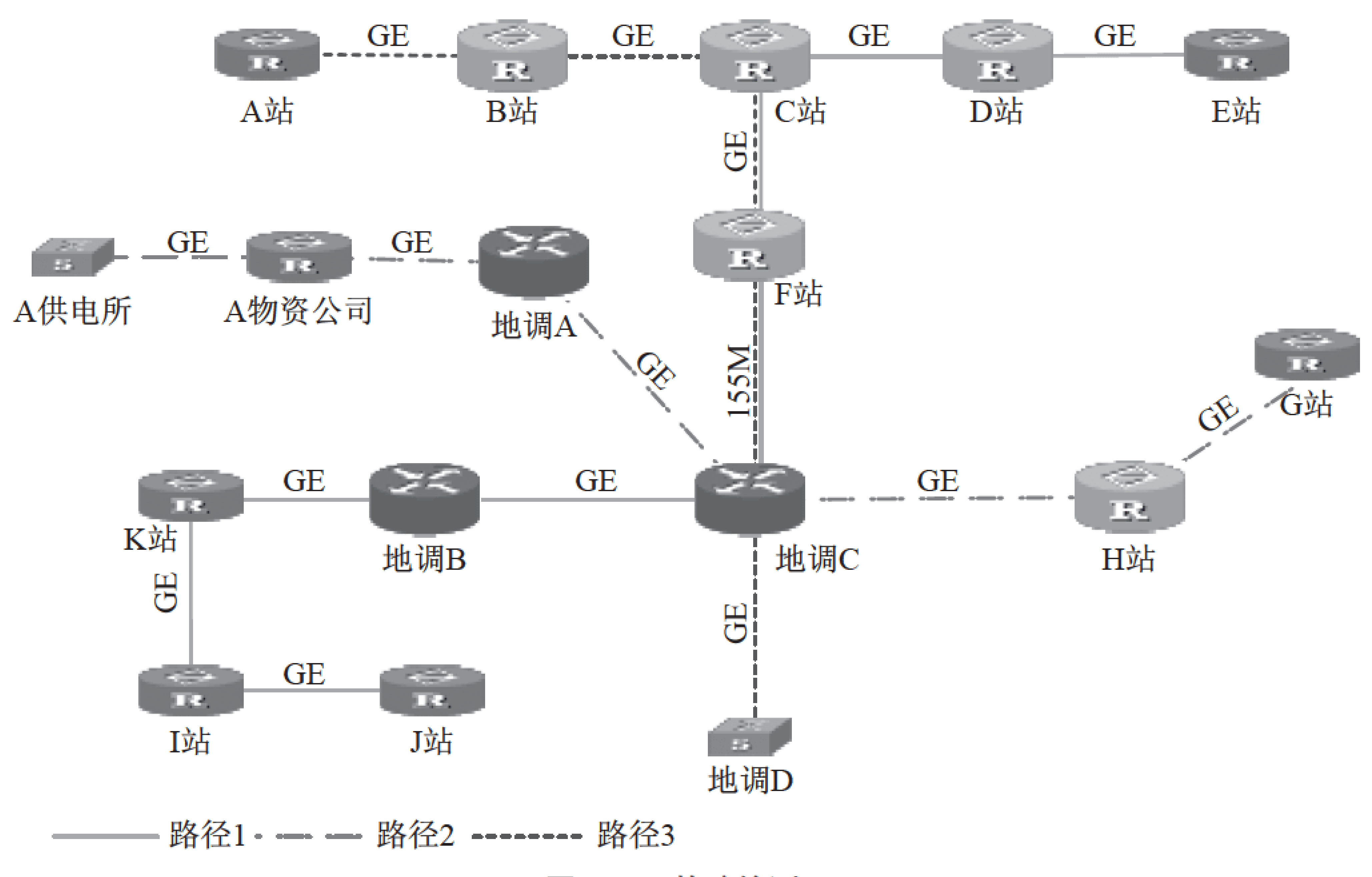


图7-12　故障检测

步骤1　进行故障检测。即先对该网络的3条网络测试路径进行检测，在A站ping E站；在G站ping A供电所；在地调D ping A站。若只有地调D ping不通A站，其他两个都能ping通，根据上述所讲的确定故障范围和缩小故障范围的技术可以将故障范围确定为：地调D—地调C和C站—B站—A站可能存在网络故障以及地调D、C站、B站可能存在设备故障。

步骤2　故障定位。首先测试网络，在A站traceroute高山楼；在高山楼traceroute C站；

在地调D traceroute地调C。若只有D—地调C测试成功，则说明地调D—地调C这段网络以及地调D、地调C都没有故障。然后对A站、B站、C站进行设备故障检测，分别在各自设备ping 172.0.0.1，若A站和C站都能ping通，而B站出问题则说明B站的路由器设备发生故障；若全部能ping通，则说明在C站—B站、B站—A站这两段发生网络故障；若A站和B站都能ping通，而C站出问题则说明C站的路由设备和A站—B站这段网络都发生了故障，如图7-13所示。

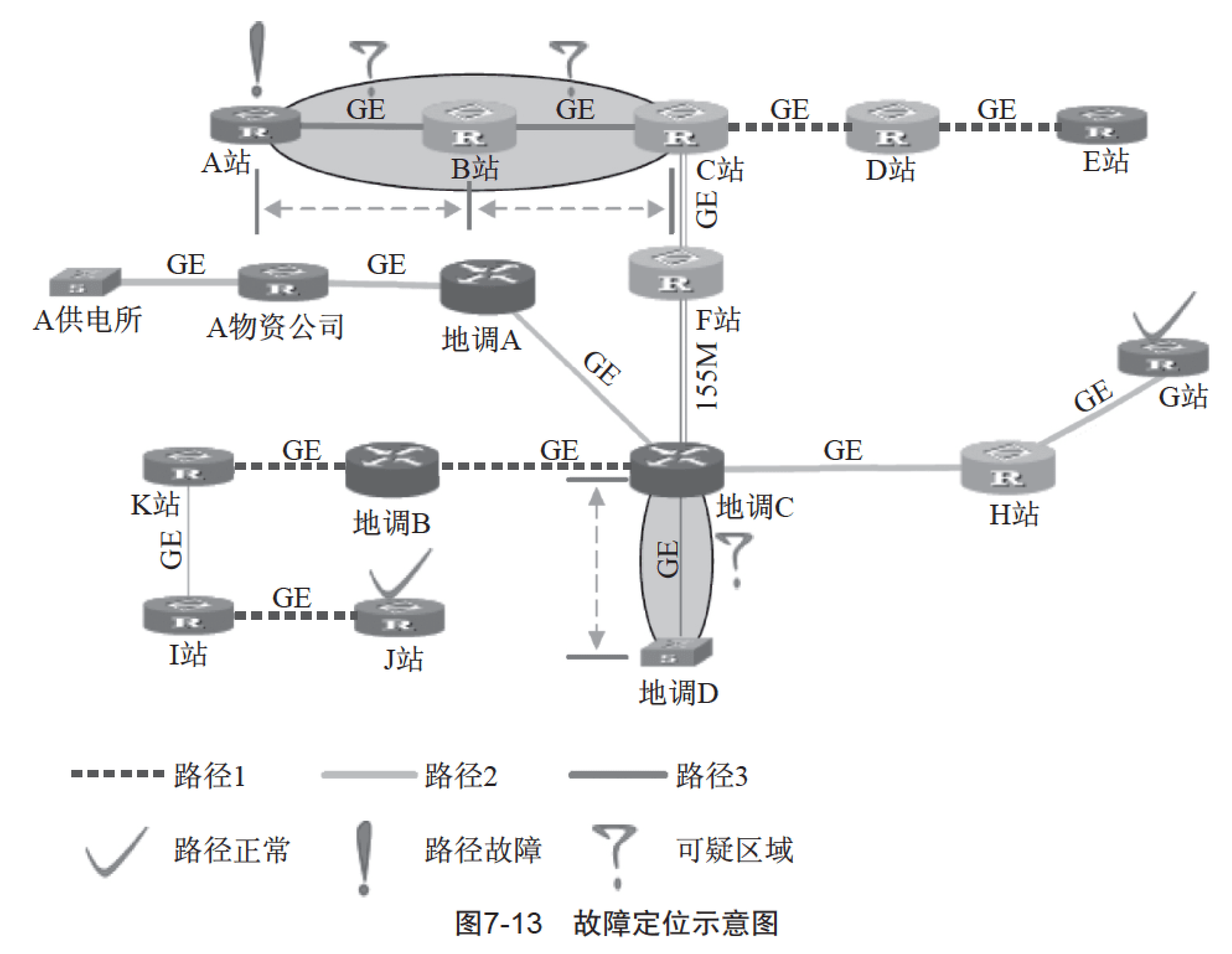


图7-13 故障定位示意图

2. EPON网络的故障探测

1）EPON接入网内部网络层测试场景

EPON内的探针之间相互进行网络层测试场景如图7-14所示。EPON探针间定期拨测流程如图7-15所示。

部署于OLT的探针会定期向部署于其下ONU的探针发起网络层拨测，反之亦然。当任何一个探针发出的ICMP请求在固定时间内没有回应时，将启动网络层拨测任务中的第二个任务，分别向部署于同OLT下的其他ONU的探针发起traceroute命令，判断到网络通道哪一段路由出现了问题。

部署于OLT的探针还会定期向部署于其他OLT的探针发起网络层拨测，当探针发出的ICMP请求在固定时间内没有回应时，将启动网络层拨测任务中的第二个任务，分别向部署于其他各OLT的探针发起traceroute命令，判断到网络通道哪一段路由出现了问题。

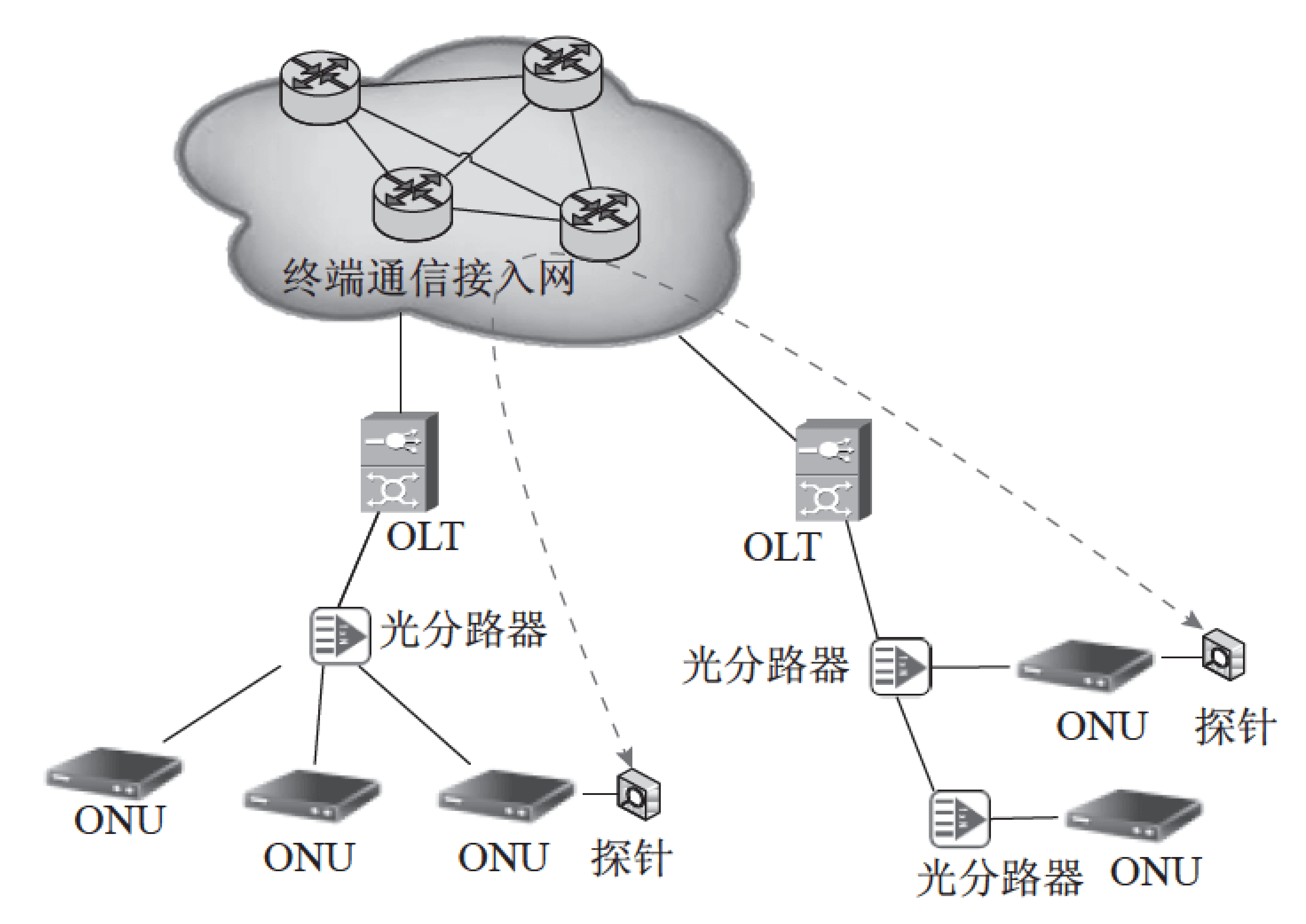


图7-14　EPON内的探针之间相互进行网络层测试场景

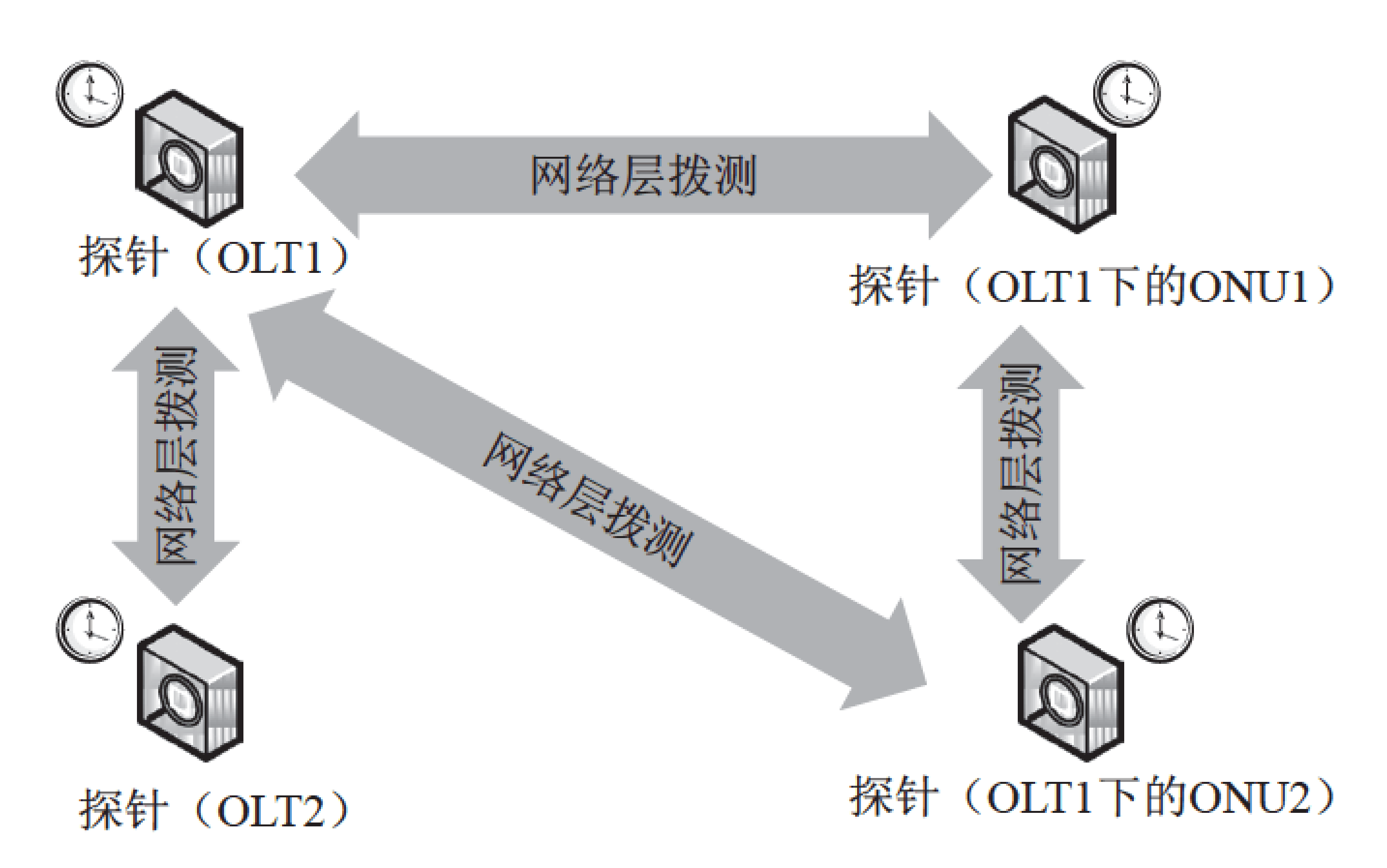


图7-15　EPON探针间定期拨测流程

2）分布式终端访问不了应用服务器故障分析场景

终端通信接入网的分布式终端如配电自动化终端、用电信息集采终端、分布式电源、电动汽车充电站访问其应用服务器如果发生故障，首先需要确认的是终端本身是否发生故障，然后再确定网络是否发生故障，如图7-16所示。

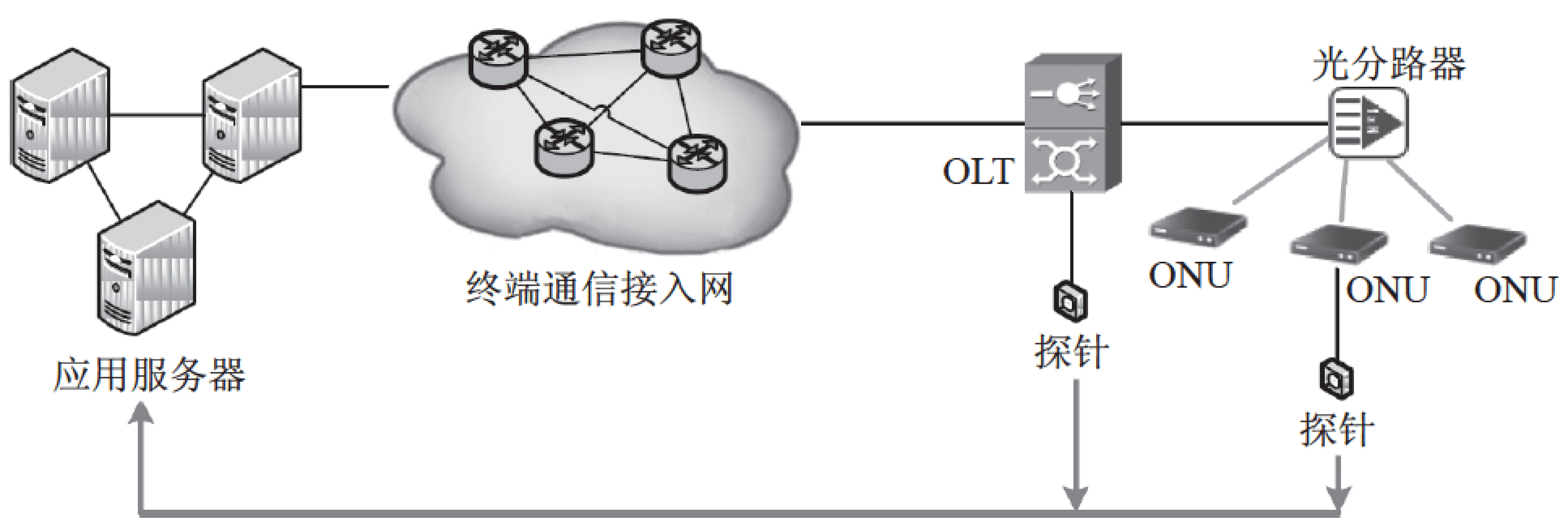


图7-16　终端通信接入网分布式终端访问应用服务器

如图7-17所示，当分布式终端访问不了应用服务器（①）时，管理人员接收到故障上报将手动调度。

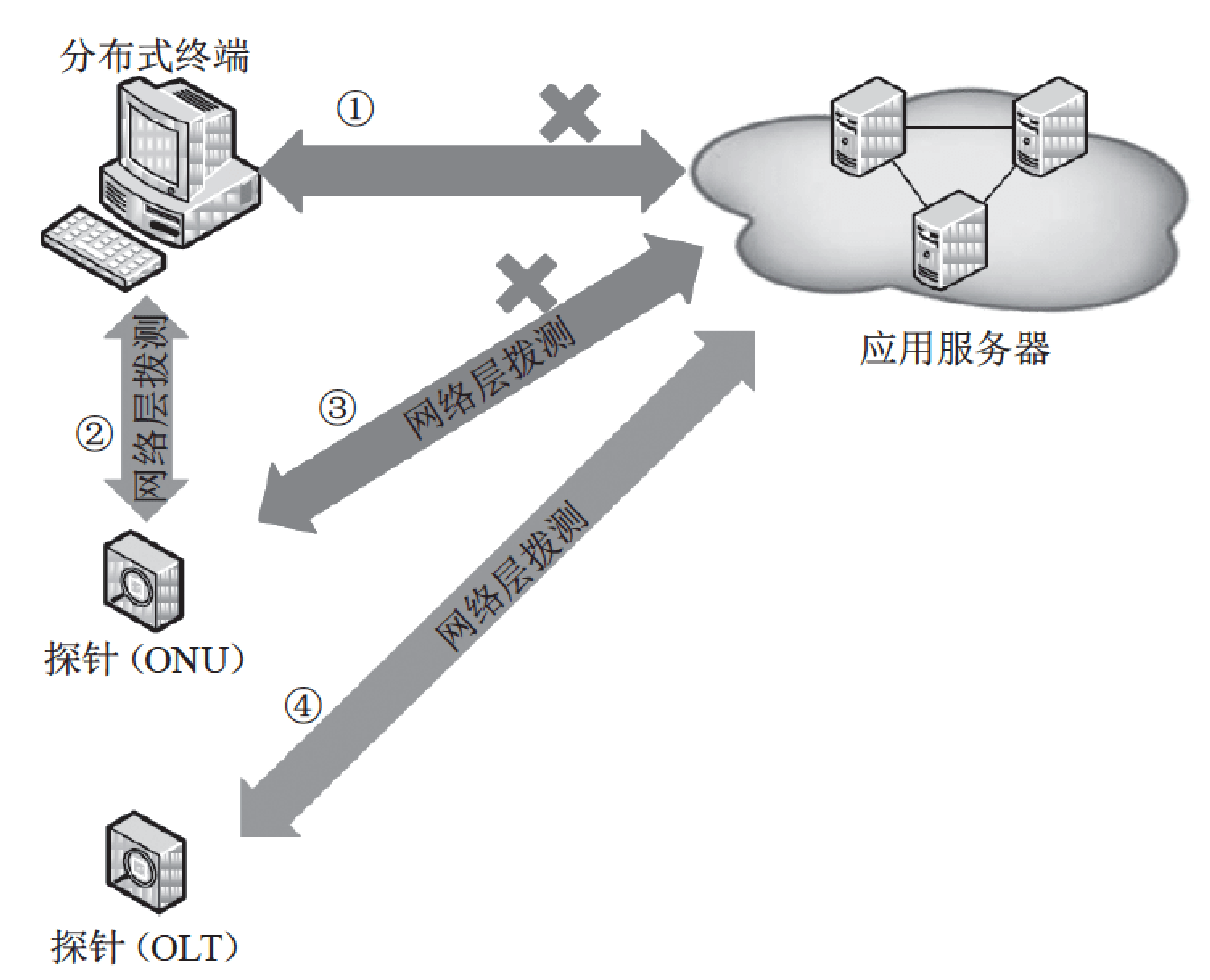


图7-17 分布式终端访问应用服务器失败场景

部署于发生故障的分布式终端所在ONU的探针向终端（②）和应用服务器（③）发起网络层拨测，确定故障发生在分布式终端还是在通信网络；若故障发生在通信网络，则调度部署于OLT的探针向应用服务器发起网络层拨测（④），确定通信故障是发生于EPON网络内，还是EPON网络之上。

3. 可编程环境下的业务自愈切换

如图7-18、图7-19的可编程环境下配电业务导向结构图和实物图所示，原来的配电业务导向是从配电主站（客户端）出发，分别向下接入无线、EPON、工业以太网进一步进行业务传输。无线从TD-LTE基站（LTE核心网）接入CPE（无线终端接入设备），然后接入HUB（集线器），最后进入DTU（服务器端）；EPON接收到配电主站的信息后，从OLT到ONU，接着进入HUB，最后进入DTU。但是在可编程环境下，在最上层加入一个管控系统，这个管控系统不但可以监视整个网络拓扑结构中的所有节点，监督节点的状况，对整个网络实现可视化，还可以对整个网络进行自动控制。

从图7-20、图7-21可编程环境下配电业务的自愈切换就可以看出，加入管控系统后整个配电网络的自愈能力大大提高。如果EPON网络任意环节出现不通的情况时，管控系统接收探针发送了反馈之后，监测到故障出现的位置，然后向LTE核心网发送指令，让业务以无线的方式进行传输；同理，当管控系统监测无线的任何一个环节出现故障的时候，也会发送一个指令给EPON，使得业务可以从EPON网络传输，工业以太网的情况同理。因此在可编程环境下网络的自愈能力大大提高。

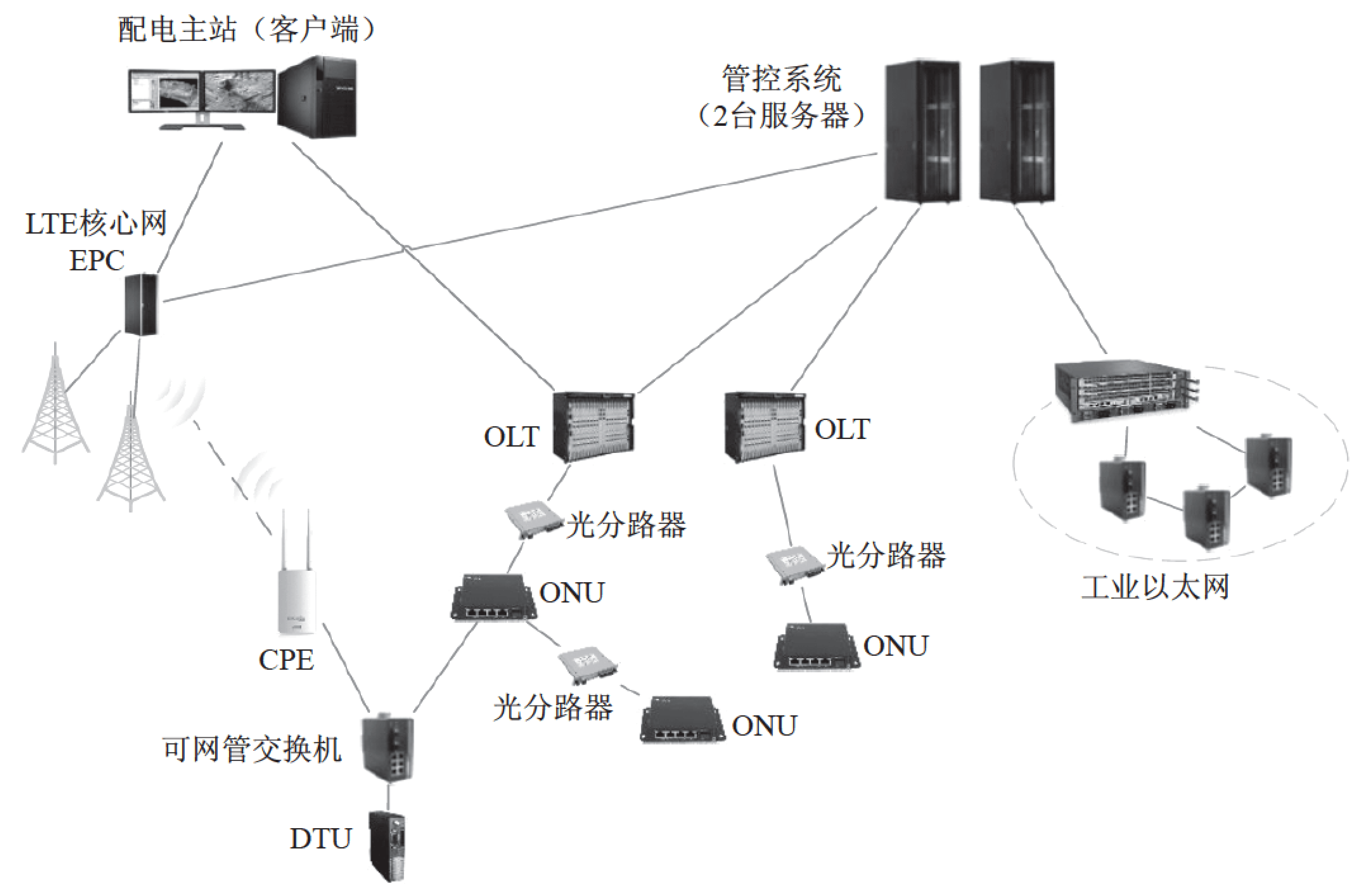


图7-18　可编程环境下配电业务导向结构实物图

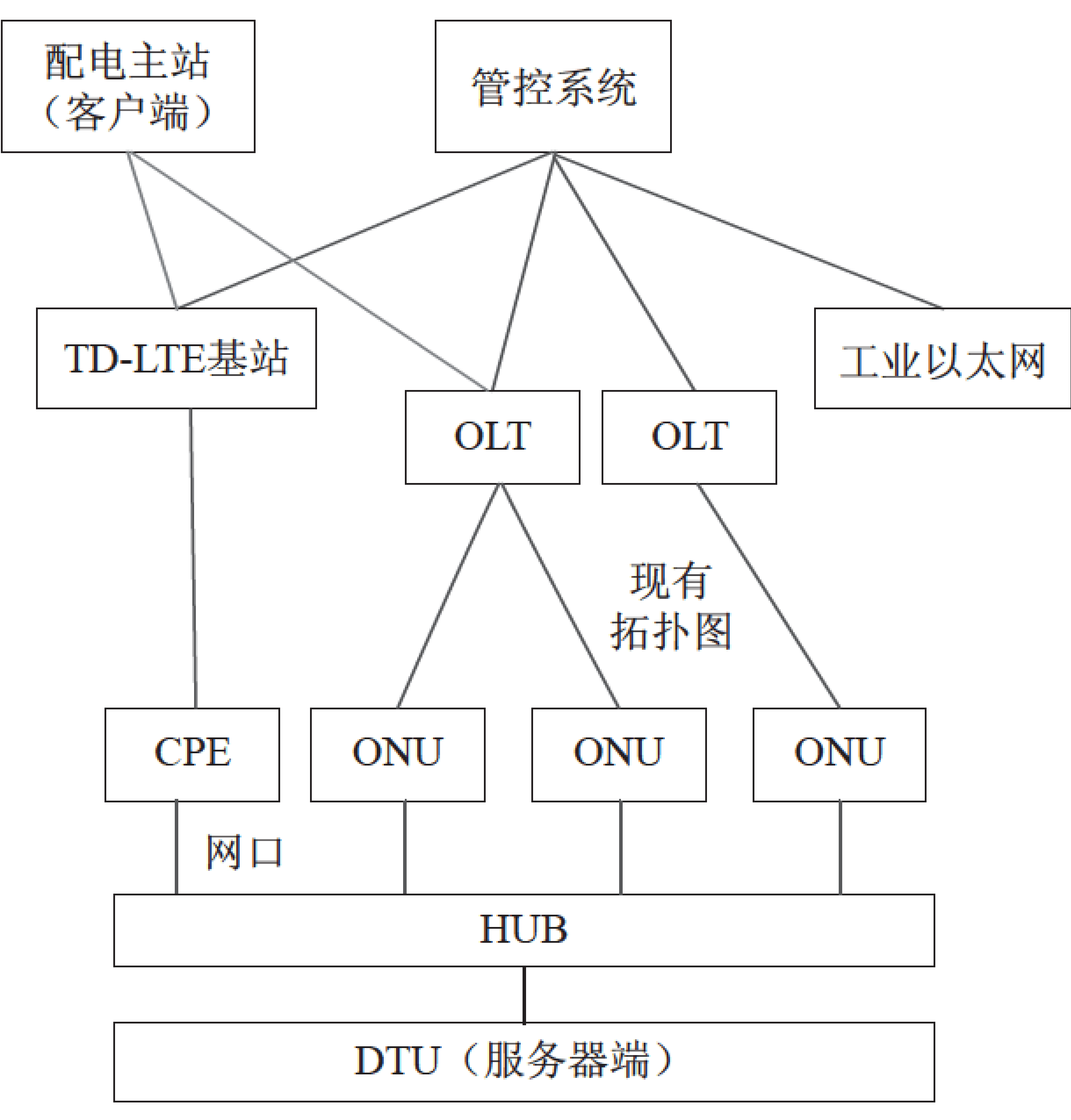


图7-19　可编程环境下配电业务导向结构图

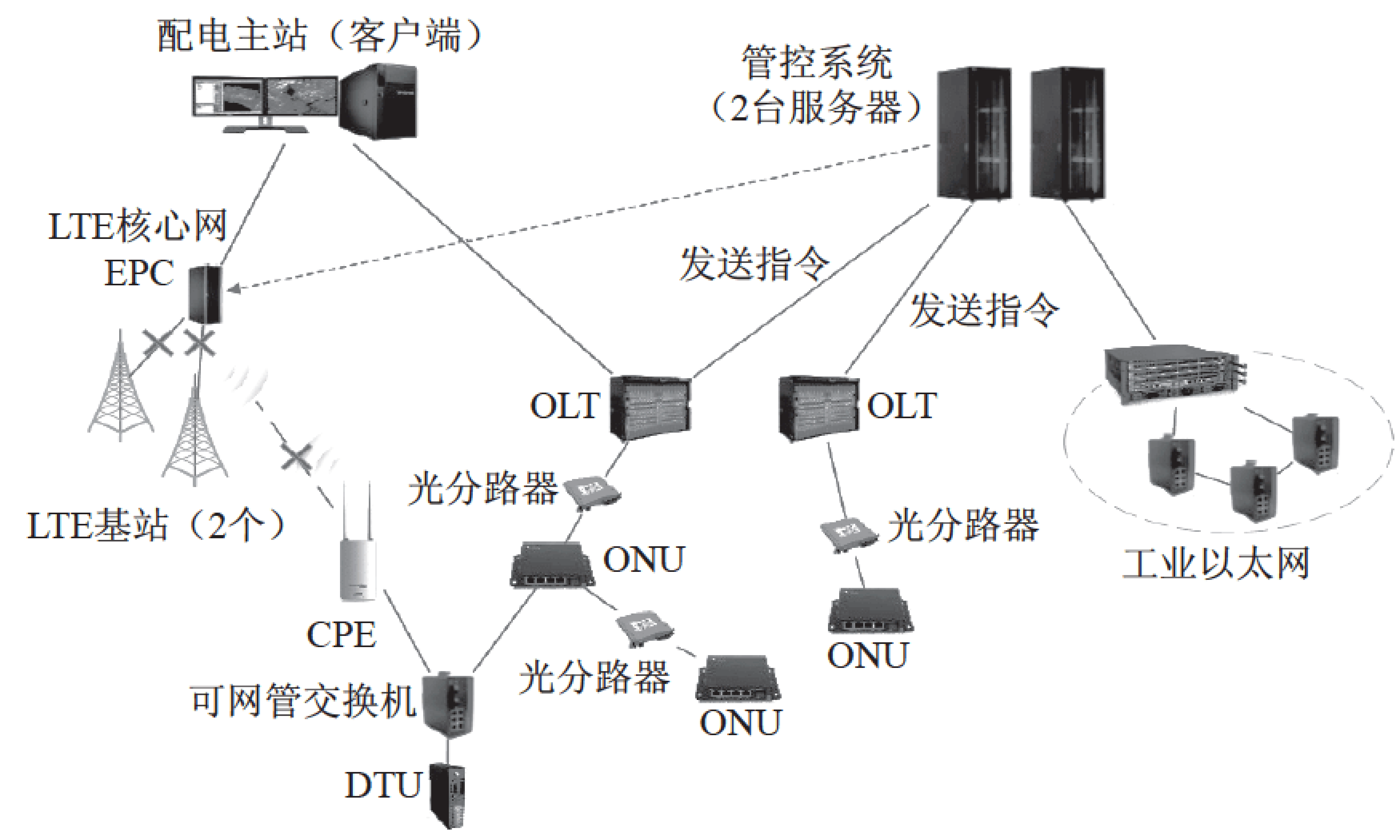


图7-20　可编程环境下的配电业务自愈切换实物图（从无线转向EPON）

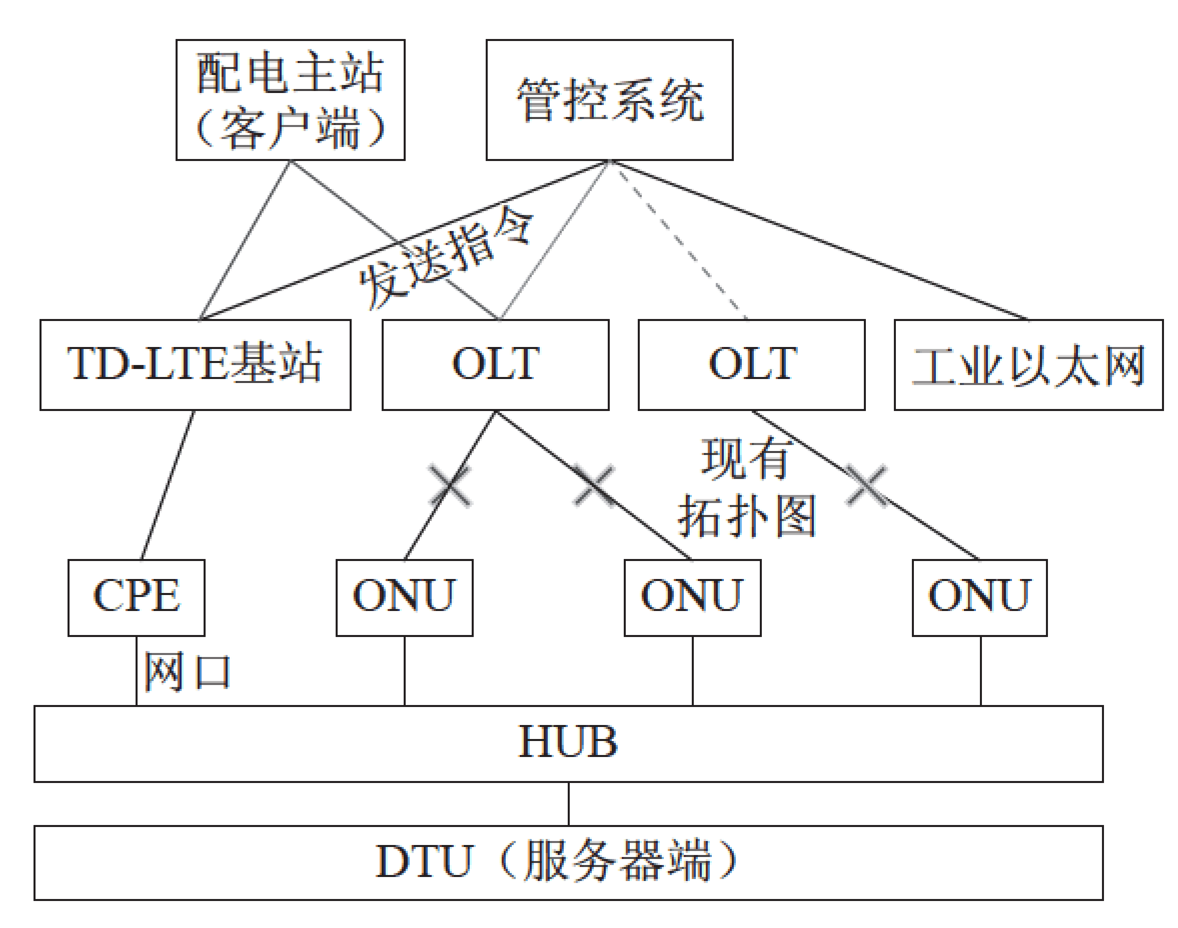


图7-21　可编程环境下的配电业务自愈切换结构图（从EPON转向无线）

7.6.2　典型场景探针部署模式

1. 典型应用场景下被动式流量采集点和采集面设置

在对各通信节点的流量分析完成之后，需要进一步计算各链路上的双向业务流量。在分析总结配电网和用电系统通信节点需求的基础上，首先需要按照各类业务的应用特点与数据流向，将变电站与各个通信节点划分出多个流量采集点和采集面，并对各个采集面业务组成及基础业务流量进行分析、测算，然后进行汇总。在进行流量计算时，应该与业务种类、业务特点和业务数量有关，而并不关注具体的路由和通信方式。

配用电业务通信节点是指与调度中心主站或调度中心有关应用系统之间有数据通信的配网终端、用电终端、配电网和用电系统监控数据采集终端及营业所各类应用系统节点；

通信节点业务流量是指上述节点或系统的数据通信业务流量；采集面是指在配电网及用电系统中与变电站具有数据通信或穿通业务的各类通信节点集合；业务采集面承载的所有业务流量总和为采集面流量。

按照智能配电网和用电系统的业务数据流向，参照已有的研究成果，可以建立配用电通信业务面及业务流向模型。配用电通信网与变电站之间包括三类业务面：业务面S1，即用电信息采集点—变电站业务面；业务面S2，即配电信息采集点—变电站业务面；业务面S3，即营业所—变电站业务面。

2. 典型应用场景下主被动探针结合部署

以配电自动化系统为例，探针设备部署于变电站汇聚设备处，运维支撑工具部署于配电自动化主站附近或者通信机房，每地市部署一套运维支撑工具，探针设备根据需要部署。可以采用主被动监测结合的方式，主动探针部署于汇聚设备处，用于监测端对端业务质量，但是链路中转接与路由设备情况难以获知，当探测到故障时，开启部署于链路重要节点的分布式硬件探针，用于进行故障定位，如图7-22所示。

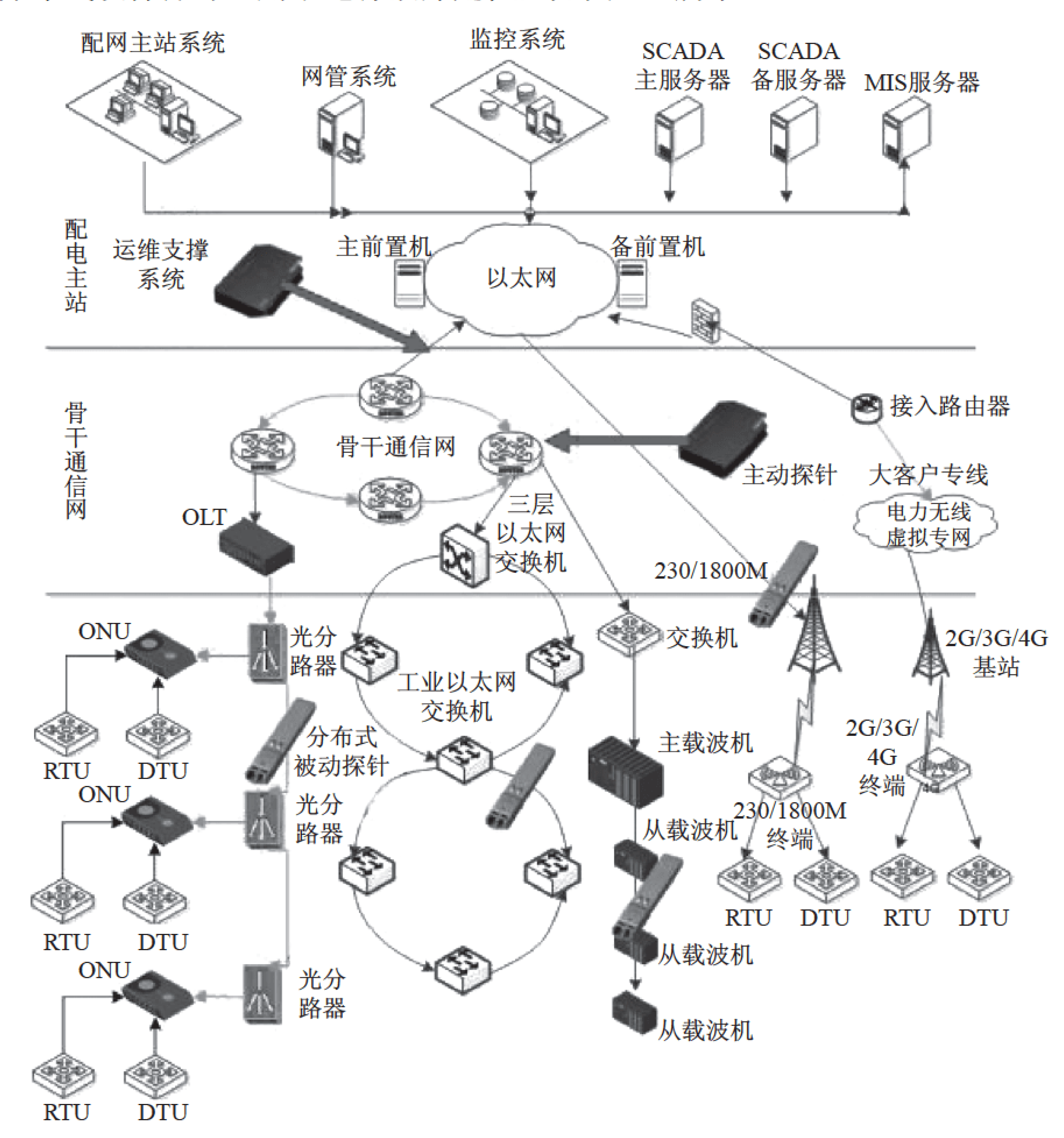


图7-22　配电自动化业务场景探针部署示意图

7.7 面向资源优化的分布式智能测量探针监控部署策略

分布式智能测量探针管控研究，作为主被动测量设备的控制逻辑，决定了网络数据平面设备部署的资源利用率，对用户业务的感知测量深度以及对动态业务的测量调度的灵活性。

电力数据网分布式探针部署问题可以分为流量监测探针部署及连通性监测探针部署两个业务需求。其中，流量监测是通过合理部署被动测量探针的方式，使用尽可能少的探针就能够监视整个网络中的流量信息；连通性监测是通过合理部署主动式探针实现端到端的主动测量，使用尽可能少的探针且测试次数尽量少的情况下，能够检测整个网络的连通性能。本节针对这两类需求，分别研究基于弱顶点覆盖的流量监测探针部署模型和基于集合覆盖的连通性监测探针部署模型，借助这些模型，运用相应的优化算法求解探针部署位置及相应的探测路径集。

7.7.1 被动式流量监测探针部署

1. 部署问题

针对电力数据网网络流量监测的业务需求，可以在网络中某一节点设置探针得到与这一节点相连的所有链路上的流量。因此，为了得到网络中所有链路的网络流量，一般可以通过在某些交换节点（如路由器）配置探针来实现。需要考虑的问题是：在网络哪些节点上设置探针，才能使得在可以得到每一条链路流量的条件下，所需流量探针数目最小。

目前一般使用最小顶点覆盖的探针部署方案解决这一问题。顶点覆盖问题已被证明是NP完全的，只能用近似算法算出近似最优解。基于最小顶点覆盖的探针部署方案能求得最小顶点覆盖的最优解，但其计算复杂度高，花费时间长，并不能应用到大规模问题中。而且最小顶点覆盖的最优解并不一定是网络流量监测探针部署的最优解，所以为了找到算法更简便，耗时更短，而且使用探针数更少的部署方案，可以结合网络流量守恒的性质通过最小弱顶点覆盖来部署探针，用更少的探针来实现整个网络的网络流量监测。

对于流量监测探针部署的评估指标包括两部分，一为部署的探针个数，二为链路覆盖率。

2. 模型建立

在网络中的关键节点设置流量监测探针可以得到与这一节点相连的所有链路上的流量。因此，为了得到网络中所有链路的网络流量，一般可以通过在某些交换节点（路由

器）配置监测探针实现。需要考虑的问题是：在网络哪些节点上设置探针，才能使得在可以得到每一条链路流量的条件下，所需流量监测器数目最小。

使用最小顶点覆盖可以解决这一问题。顶点覆盖问题已被证明是NP完全的，只能用近似算法算出近似最优解。在考虑到网络监测方式的同时，加上流量守恒的约束，使用最小弱顶点覆盖能够部署更少的探针来实现整个网络的网络流量监测。同样，最小弱顶点覆盖问题也已被证明是NP完全的，也是只能使用近似算法求近似最优解。

首先将网络拓扑图转化为无向图 $G(V,E)$，其中 $V=(v_1,v_2,\cdots,v_n)$ 为网络节点集（在IP网络中可看作路由器），$E=(e_1,e_2,\cdots,e_m)$ 为网络中的链路集合。其中，$n=|V|,m=|E|$ 分别表示G中节点和链路的数目。用 $e_k=(v_i,v_j)$ 表示 e_k 是连接节点 v_i 和 v_j 的一条链路。然后将网络中的各个设备按照顺序进行标号，统计全部设备和链路信息。

根据以上网络模型，给出如下定义：

定义1：给定无向图$G(V, E)$，其中V是顶点集，E是边集，S是V的子集，若根据与S中顶点相关联的各条边的流量，可以确定E中任意边的流量，则称S是图G关于流量的测量集。

定义2：给定一个无向图$G(V, E)$，求顶点集V的一个最小子集S，使得 $e=(u,v)\in E$，且$u\in S$或$v\in S$，即E中的任一边至少含有此子集中的一个点作为顶点，也就是说S中的顶点覆盖了边集E。

最小顶点覆盖问题已被证明是NP完全的，到目前为止还不存在多项式时间算法来求解，可以用贪心算法去求出近似最优解，即每次迭代都选取度最大的节点作为探针，然后所有与其相连的节点都可以排除掉，满足每次选取探针都是当下情况的最优情况。但是考虑到每次的最优并不一定能得到整体上的最优，为了找到更小的解，通过下面的限定策略，对贪心算法进行改进，通过分支界限法来得到更优解。

3. 模型求解

算法步骤如下：

步骤1　对所有节点度排序，取前k个节点，当其满足

$$\begin{cases}\sum_{i=1}^{k-1} Degree(Vi) < |E| \\ \sum_{i=1}^{k} Degree(Vi) \geqslant |E|\end{cases}$$

时得到最小可能k。

步骤2　将原图数据构造成一个解空间树的节点，利用定界策略判断是否有解，如果无解将k加1，重新进入步骤2，如果有可能有解则插入到优先队列中。

步骤3　若优先队列不为空，那么便从优先队列中取出第一个可行的节点，进入步骤4，如果优先队列为空则将k加1，重新进入步骤2。

步骤4　判断当前节点是否满足解的条件，如果满足便输出解并退出，如果不满足便进入步骤5。

步骤5　检查当前节点是否可以扩展，不能扩展便进入步骤3继续循环，如果能扩展则扩展。然后验证扩展到左右节点是否有解，将有解的扩展节点插入到优先队列中，然后进入步骤3继续循环。

7.7.2　主动式网络连通性监测探针部署

1. 部署问题

网络的连通性测试需要获得端到端的网络性能，因而采用主动测试的方式部署探针，考虑到现实中网络规模可能较大，为减轻网络的负担，可以选取基于ICMP协议的ping命令来获得网络中端到端路径的连通性，并配合使用traceroute命令进行故障诊断。针对主动测试的端到端的测试方式，考虑到减少主动测试给网络带来额外负担的影响，这里提出了基于集合覆盖的探针部署方案，在考虑了部署尽量少的探针的同时，考虑使用更少的测试路径以减少额外的网络负担。

网络连通性测试探针的部署评估指标包括：ⓐ部署的探针的个数；ⓑ测试路径条数；ⓒ链路覆盖率。依据求解问题的特征，这里将连通性监测的探针部署抽象成最小集合覆盖模型。最小集合覆盖问题得到了大量研究并广泛应用在软件测试、模式识别、生物信息学等领域，是一个经典的NP完全问题。解决此问题的方法主要有贪心算法及启发式搜索算法两大类。贪心算法实现容易，计算时间较后者快很多，但是无法保证解的最优性；启发式搜索算法可以通过局部搜索最优解求得比贪心算法质量更高的全局范围内的优化解，但实现复杂度高，运算时间比较长。考虑到探测的实时性，这里拟选择贪心算法作为模型求解的算法。

确定了探针集以及相应的测试路径后，在实际监测时首先根据测试任务列表确定测试目的节点，然后按照一定的频率ping各个目的节点，采集一定时间内的数据评估连通性状况并收集返回的结果。如果发现有测试路径无法连通，则进行故障诊断。根据已经返回的测试结果判断故障可能的位置，如果需要还可以发送traceroute辅助探针，直到最后定位出故障位置。

2. 模型建立

依据求解问题的特征，将连通性监测的探针部署抽象成最小集合覆盖模型。模型描述如下：

一个数据网可以抽象成一个无向图$G(V, E)$，其中V是网络中所有节点的集合，E是网络中节点间的通信链路集合，$|E|$，$|V|$分别表示网络中的节点数目及链路数目。定义 $P_{s,d}=\{e|e\in E,s\in V,d\in V\}$ 为节点s到d的通信路径包含的链路集合，网络中的任意两点间路径的链路集合由路由算法决定，所有路径的链路集合定义为网络的路径集合$T=\{P_{s,d}|s\in V,d\in V,s\neq d\}$，满足大小为$|T|=\dfrac{|V|(|V|-1)}{2}$，且$E$中的任意一条链路都至少包含

在T中的一条路径里。

按照集合覆盖的思想及连通性监测的覆盖要求，本模型求解的是最小的路径集合$T_s \subset T$，使得E中所有的链路都被T_s覆盖，即$\forall e_i \in E, \exists P^i_{s,d} \in T_s$，使得$e_i \in p^i_{s,d}$。

所求得的T_s即可作为连通性测试的测试路径集，$|T_s|$即为测试路径的条数。

定义V_s为待部署的探针集，它包含了T_s所有测试路径的两个端点，即：

$$\forall P^i_{s,d} \in T_s \text{都有} s, d \in V_s,$$
$$\text{且} \forall v \in V_s, \exists P^i_{s,d} \in T_s, \text{使得} v \in \{s, d\}。$$

3. 模型求解

最小集合覆盖问题得到了大量研究并广泛应用在软件测试、模式识别、生物信息学等领域，是一个经典的NP完全问题。解决此问题的方法主要有贪心算法和启发式搜索算法两大类。贪心算法实现容易，计算时间较后者快很多，但是无法保证解的最优性，启发式搜索算法可以通过局部搜索最优解求得比贪心算法质量更高的全局范围内的优化解，但实现复杂度高，运算时间比较长。这里选择贪心算法作为模型求解的算法。

1）数据预处理

对数据网拓扑图，按照从内到外、从骨干核心层到接入层的顺序进行编号。按照点到点的格式表示出图中的每一条链路，完成数据的准备。

依据模型假设需要对数据进行裁剪。这里采用两种不同的裁剪方式，第一种是选择路由器或交换机等大型的数据交换设备形成一组数据；第二种是除去接入层构成另一组数据。

2）算法流程

鉴于上述最小集合覆盖模型，设计其贪心算法流程如下：

步骤1 计算网络中任意两点间的最短路径作为点到点的路由线路$P_{s,d}$，可使用经典的Floyd算法或Dijkstra算法。

步骤2 初始化网络中任意两点间的路由线路的未被覆盖链路数$U_{s,d}$为该线路的长度$|P_{s,d}|$。

步骤3 求出当前网络的路由线路中未被覆盖链路数$U_{s,d}$最多的那条线路$P_{\max}$，若存在多条这样的线路，则选择端点已被选为探针的数目多的那条线路。

步骤4 把$P_{\max}$加入最小路径集T_s，同时将$P_{\max}$的两个端点加入探针集V_s。

步骤5 将$P_{\max}$中包含的所有链路标记为已覆盖，同时更新网络中任意两点间的未被覆盖链路数$U_{s,d}$。

步骤6 若网络中的所有链路都被覆盖则结束，否则返回步骤3。

算法流程图如图7-23所示。

开始

求网络中任意两点间的最短路径，将其作为两点间的路由线路$P_{s,d}$

初始化任意两点间的未被覆盖链路数$U_{s,d}$为其路由线路的长度$|P_{s,d}|$（假设链路长度为1）

求出当前$U_{s,d}$最多的一条路径$P_{\max}$，若有多条这样的路径，则选择端点已被选为探针的数目多的那条路径

把$P_{\max}$加入最小路径集T_s，同时将$P_{\max}$的两个端点加入探针集V_s

将$P_{\max}$中包含的链路标记为已覆盖，同时更新网络中其他路径的$U_{s,d}$

所有的链路都被覆盖？

N

Y

结束

图7-23　基于集合覆盖的连通性监测算法流程图

7.8　基于主动探测技术的故障定位

7.8.1　主动探测技术逻辑部署

1. 拨测对象

拨测代理所测试的对象包括：

① 以无线质量回传和机房数据通信网内的网络设备（路由器和交换机）进行网络层测试。

② 以办公室和地区数据通信网内的网络设备进行网络层测试。

③ 以机房数据通信网间的网络设备进行网络层测试。

2. VPN拨测方式

拨测终端需要连接到各个不同的VPN中访问相应的服务器系统模拟实际业务，对流量

进行测试。建议未来可部署多个拨测终端分别对应各个VPN配置网口，其管理端口则连接到全局路由中，以实现数据传递至管理平台，整体部署逻辑示意图如图7-24所示。

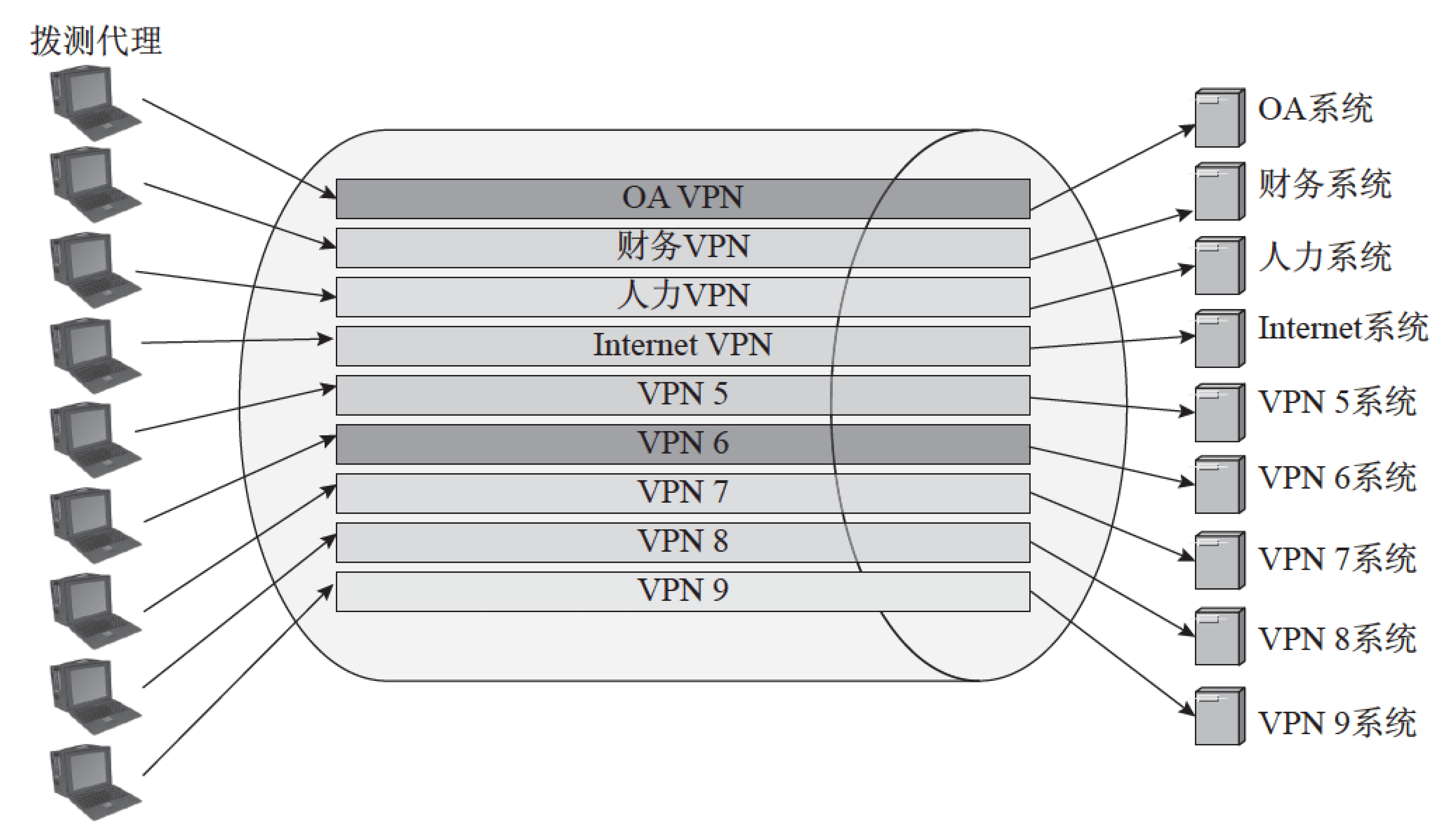


图7-24　拨测代理部署逻辑示意图

拨测子系统的另一个功能是可以记录网络层测试目标的路由路径及跳数，针对测试目标路由变动查询有所帮助。目前数据通信网组网结构是通过MPLS VPN方式承载不同的业务流量，由于在MPLS标签交换环境中无法通过拨测路径测试获得具体路由路径，但数据通信网全局路由是完全的IP路由交换，并不经过任何MPLS VPN，因此可以通过拨测全局路由测试获得具体路由路径。如果针对相同目标，同时测试VPN和全局IP地址，通过全局IP的路由路径可关联出VPN地址中的路径。拨测方式示意图如图7-25所示。

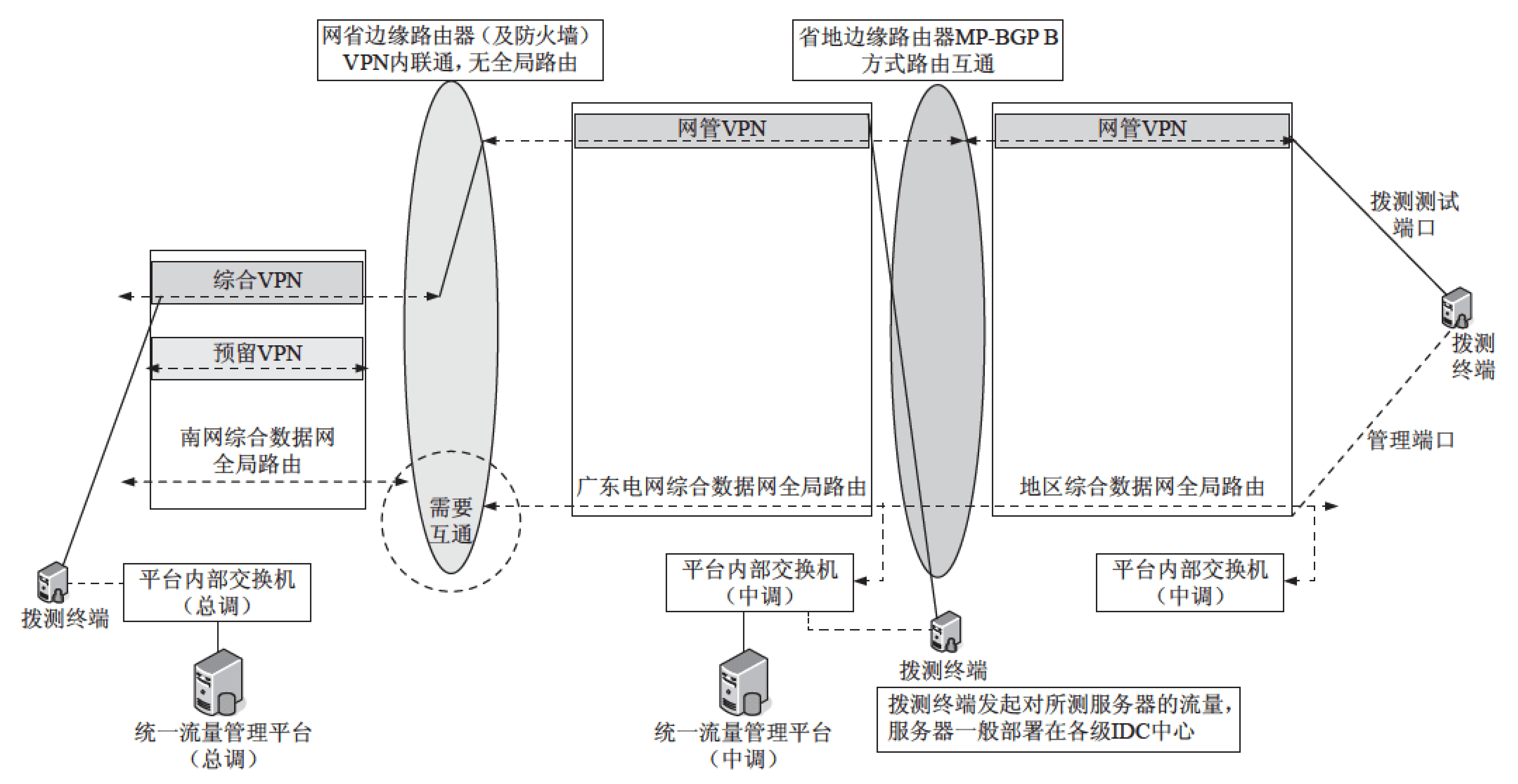


图7-25　拨测方式示意图

3. 拨测任务流程

网络层拨测任务流程如图7-26所示。

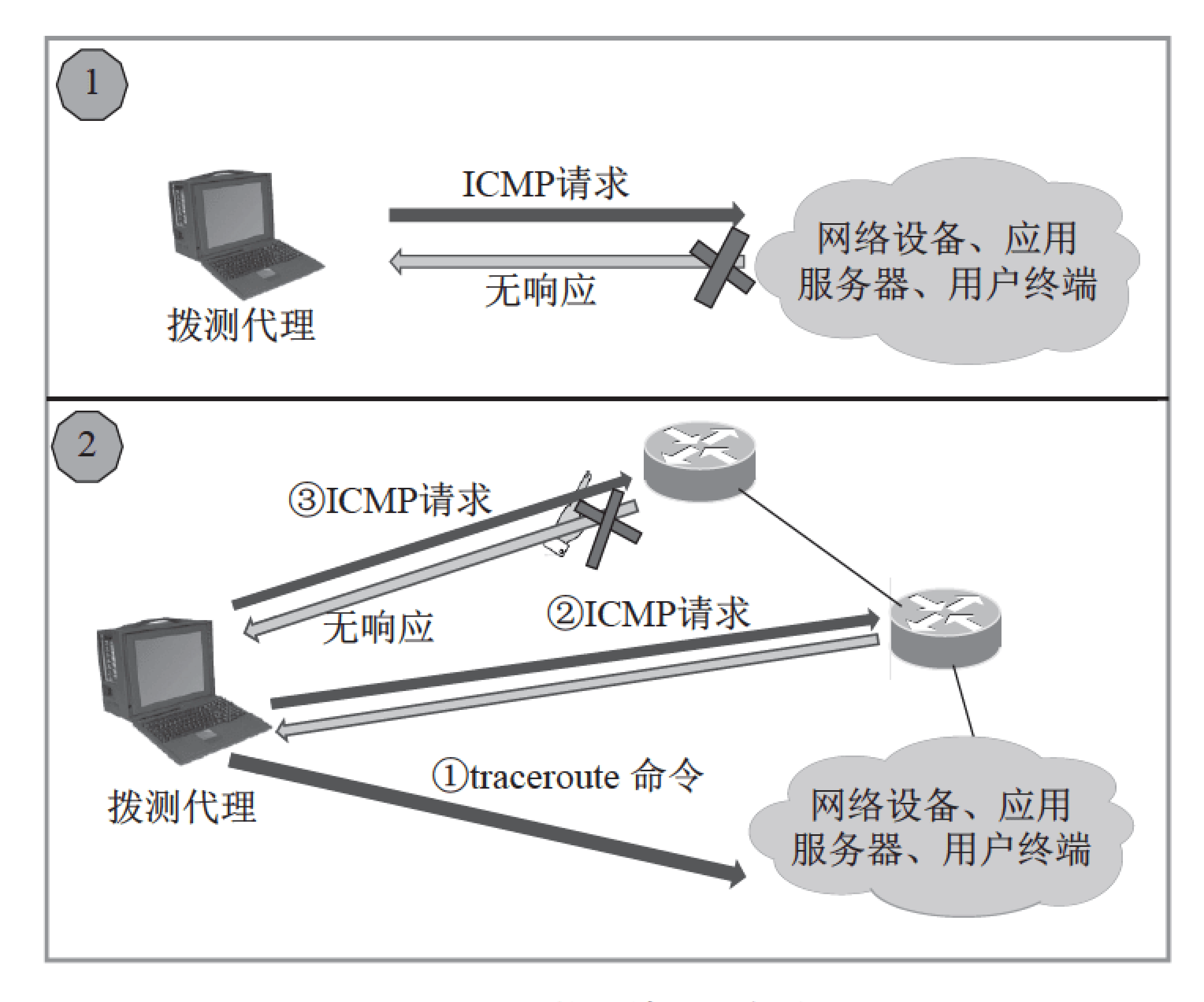


图7-26　网络层拨测任务流程

网络层拨测任务流程包括以下两个过程：

① 拨测代理向网络设备、应用服务器以及用户终端发起ICMP请求时，在固定请求次数内，拨测对象没有响应时，拨测代理初步判断网络不可达，将进入下一个测试流程。

② 拨测代理向网络设备、应用服务器以及用户终端发起traceroute命令（①），拨测代理会对每一跳路由进行ICMP请求（②③），当某一段路由无响应时，将该段路由的IP提示出来（③）。

应用层拨测任务流程包括TCP连接失败任务流程和业务连接失败任务流程。其中，TCP连接失败任务流程如图7-27所示。

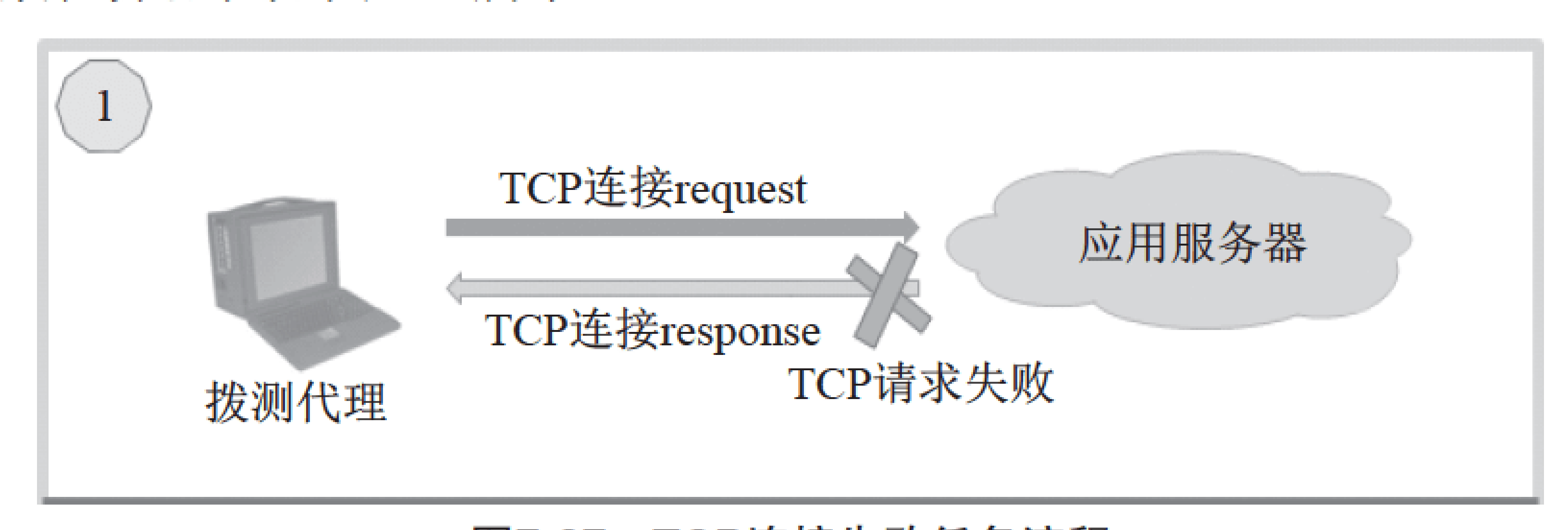


图7-27　TCP连接失败任务流程

当拨测代理向应用服务器发起的TCP会话连接失败时，拨测代理将提示出TCP请求失败的具体原因。

业务连接失败任务流程如图7-28所示。

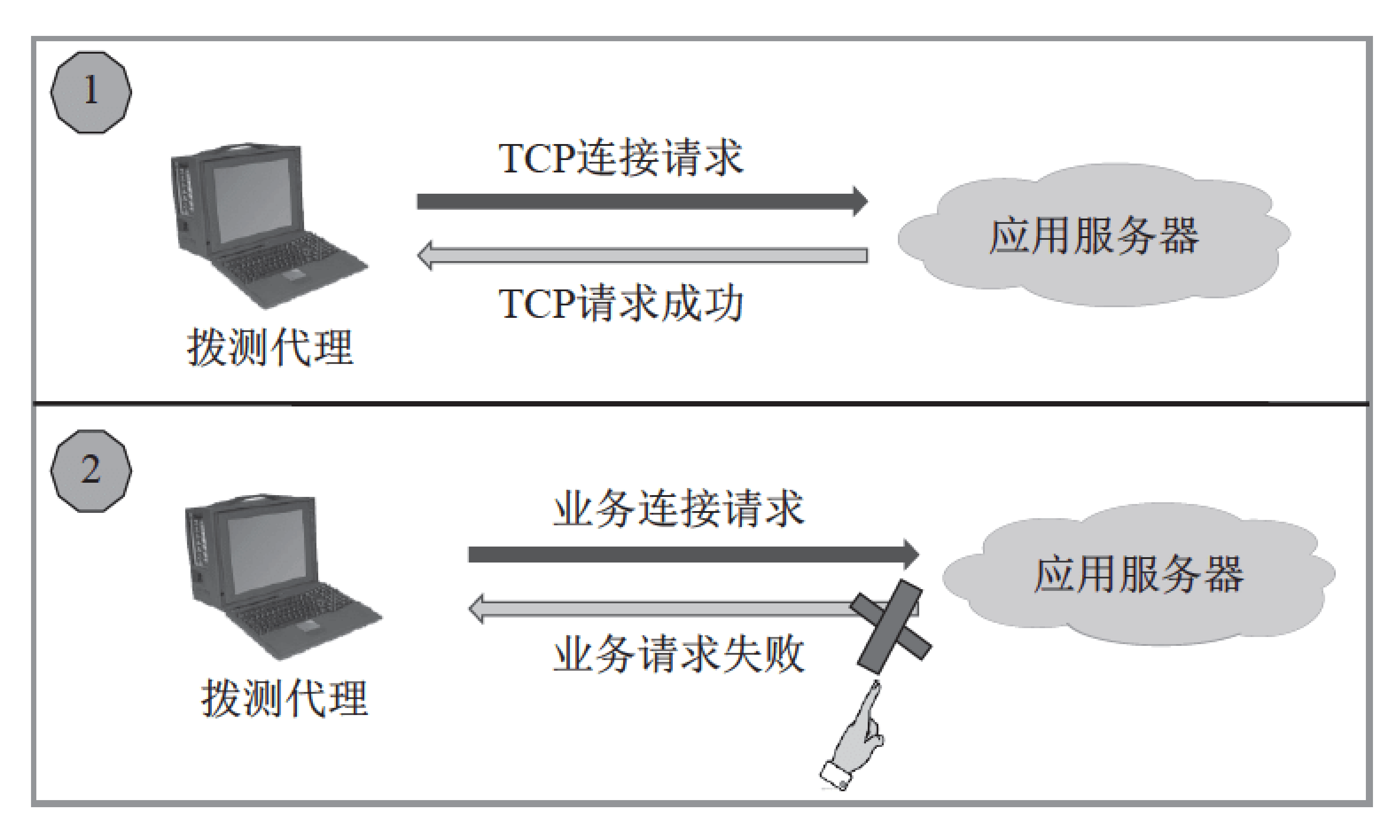


图7-28　业务连接失败任务流程

① 拨测代理向应用服务器发起TCP连接请求成功时，将进入下一个测试流程。

② 拨测代理向应用服务器发起业务连接请求失败时，拨测代理将提示出业务请求失败的具体原因。

4. 探针接入方式

如图7-29所示，探针设备通过两个RJ45以太网端口与路由器直连，具体说明如下：

① 管理口，配置唯一全局路由地址，Access类型。

② 测试口，通过子接口设置多个VLAN，每个VLAN对应一个业务VPN。需分配多个VLAN地址，Trunk类型。

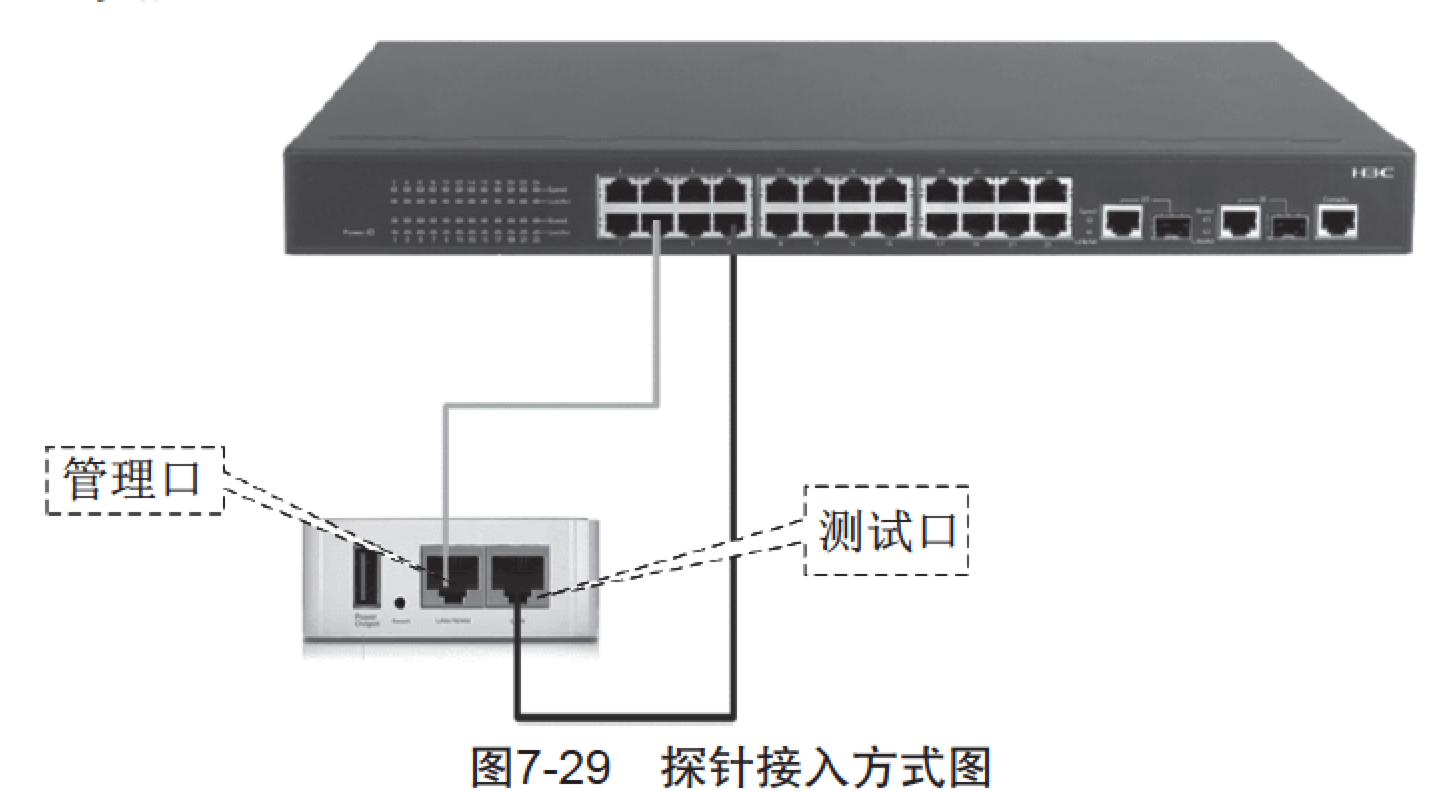


图7-29　探针接入方式图

路由器同时需提供两个RJ-45以太网端口，具体说明如下：

① 管理口走VPN带外全局路由，Access类型。

② 测试口通过设置子接口设置多个VLAN，每个VLAN对应一个业务VPN，VLAN号建议与VPN VLAN设置一致，Trunk类型。

所以，在部署的过程中，为每个探针分配2个IP地址，一个IP地址分给管理口，另一个IP地址分给测试口。

7.8.2 故障定位的原理

解决故障定位问题的方法多种多样，它们的理论基础大致相同，均来自人工智能、信号处理、图论、模式识别、信息论等计算机科学领域。根据知识组织方式和推理机制的不同，可将目前常用的故障定位方法大致分为：基于规则推理的诊断方法、基于案例推理的诊断方法、基于模型的诊断方法、基于模糊逻辑的诊断方法等。

1. 基于规则推理的诊断方法

在基于规则的推理方法中，规则是由相关领域专家的知识与经验表示出来的，一般形式是：if<前提>then<结论>。其中，任何能与数据匹配的模型放在前提部分，满足前提时可以得出的结论放在结论部分。基于规则的推理方法是首先根据相关的推理从规则库中选择相应的规则，然后与规则的前提部分相匹配，最后根据匹配的结果得到结论。基于规则的推理系统一般由一个工作内存、一个知识库和一个推理机（即推理引擎）组成。这三部分分别描绘了系统的数据层、知识层和控制层。

工作内存中包含了收集到的各种数据信息。工作内存通过分析这些信息识别出诊断对象是否发生故障。

从人类领域专家那里得到的专家知识被放在知识库中，包括两部分内容：ⓐ关于诊断对象出现问题时定义的专家知识；ⓑ当某一特定问题发生时所要执行的动作。知识库中的专家知识是基于规则的，就是所有知识都采用“if-then”或者“condition-action”两种形式来表示。

推理机与知识库协同工作，将知识库中的规则与诊断对象进行比较，从而确定该规则能否被使用。当条件满足时，才会输出规则的后项。一种十分少见却最简单的情况是用一条规则就可以判断出诊断对象的故障。多数时候推理机需要将得到的结论作为条件在知识库中进行多次推理，才能得出最终的故障结论。

基于规则推理的方法虽然结构简单，易于实现，但是存在以下缺陷：

① 规则必须精确匹配。如果当前的诊断对象状态与规则的条件不匹配，那么系统将退出整个推理过程。

② 对每个对象的诊断需要多个规则，随着诊断对象的数量增加，相应的规则数量也会呈指数级增长，对存储规则的数据库的容量需求也将越来越大。

③ 规则不易维护。由于知识是特定于诊断对象配置，无论何时，诊断对象的相关配置变更都需要开发或改变规则。

2. 基于案例推理的诊断方法

基于案例推理的故障定位方法和上述方法有较大的区别。基于案例的推理根据以往

求解类似问题的经验知识进行推理，从而获得对当前问题求解的结果。一个有效的案例表示要包括三部分内容：案例发生的原因或背景；案例的特点或过程；案例的解决方法与结果。其思想来源于现实生活，一些事件在现实中总是重复发生，处理类似事件的方法也可以用这个方法。因此在现实生活中，我们想要解决某一问题时，可以从曾经经历过的相似例子中寻找解决方法。基于这一思想，将过去故障诊断的成功案例存入案例库，每当遇到新故障时，我们可以在案例库中寻找类似的案例，利用类比推理方法得到近似的解，再对答案加以适当修改，使之完全适合新问题。

CBR故障定位系统由五个部分组成，其中包括一个案例库和四个功能模块。首先输入模块接收诊断对象故障的描述。然后检索模块在案例库中寻找与之匹配的案例，如果有完全匹配的案例，那么要找的答案就是该案例的故障源；如果找不到完全匹配的案例，检索模块就会在案例库中找一个最相似的案例。之后由修正模块根据故障间的差异对该案例的解作适当修改，这样就可满足当前问题的要求了，其结果是得到一个完整的解。一旦找到故障源，一个新的案例就会被处理模块加入到案例库中，供以后故障定位时使用。检索模块会提供多种匹配方式来对案例进行匹配。

基于案例推理的故障定位方法克服了基于规则推理方法的许多不足：

① 在规则推理方法中，知识的单元是规则；而在案例推理方法中，知识的单元是案例。

② 在规则推理方法中，检索是基于对规则的完全匹配；而在案例推理方法中，检索是基于对案例的部分匹配。

基于案例推理的故障定位推理方法有自学习能力，在刚开始运行此方法的时候，几乎找不到匹配案例，随着运行次数的增加，案例库中存储的案例逐渐增多，相匹配的情况会越来越多。如此可知，对于故障诊断可以将二者结合起来，利用规则推理诊断方法对知识库进行预学习，在进行诊断的时候采用案例推理诊断方法保障系统的健壮性。

3. 基于模型的诊断方法

与前面所述两种方法不同，基于模型的推理方法在建立的系统模型中包含领域专家的专业知识，更多地利用系统的结构、行为与功能等知识是基于模型的诊断方法的特点。相对于基于规则的推理方法，这种诊断方法能够处理未知的情况，系统存在的潜在故障也有可能被检测到。这类方法的知识库比较容易建立且具有一定的灵活性。

基于模型诊断方法的系统模型根据系统的组成元件、功能及元件间的相互联系而建立，描述了系统的结构和功能。

诊断系统是一个三元组，包括系统描述、观测量集和组成系统的元件集合。系统模型建立是基于模型的诊断方法的核心。系统模型中的诊断对象相关信息和告警触发条件的获得及更新是难点。模型利用已经定义的行为进行告警相关性分析。如果有一些实体没有相应的模型，就需要建立新的模型，并将模型转化为相应的程序。基于模型的方法的学习和

自适应能力较差。

基于模型的故障定位方法由于所建立的模型不同，建立于其上的方法也不尽相同，如今应用较广的有基于密码本关联模型的故障诊断方法。

基于密码本关联模型（Codebook Correlation Model）的故障定位方法是，由故障源引发的事件集被视作标志故障源的“密码”，对捕获到的一系列故障事件进行“解码”就是定位故障源的整个进程。此方法不需要专家知识来将故障源和故障事件联系起来。

密码本关联模型的故障诊断方法中，故障事件被看作由原始系统产生的消息并被编码成为它们导致的普报。密码本技术有两个过程：密码本生成是第一过程，这其实是一个“问题—现象”矩阵；第二过程叫作解码阶段。

故障因果关系图描绘了故障事件间的因果关系，它是产生密码本的必须因素。每一个节点代表一个故障事件。指示线将因果事件的节点相连，起于起因事件，终于结果事件。问题节点就是入度为零的节点，其他节点为故障现象节点。从原始因果图中去掉故障现象节点间的指示线，将得到一个新的标注过的故障因果图。由删减过的因果图便可生成相应的密码本。

基于密码本关联模型的故障定位方法，其最大的优点就是不需要通过专家知识来进行故障定位。该方法定位时只需要进行比较操作，运算的复杂度较低，所以该方法在速度上有一定的优势。

4. 基于模糊逻辑的诊断方法

在基于模糊逻辑的故障定位方法中，其知识表示采用模糊产生式规则。模糊产生式规则是将传统产生式规则“if<条件>then<结论（或动作）>”进行模糊化。引入模糊的概念可以更好地模拟人类的思维与决策过程，计算机的计算结果不再是简单地从0或1中二选一，而是选择在区间[0，1]之间的一个值。

使用模糊逻辑诊断方法最重要的是建立模糊隶属度，确定隶属度的方法有许多。计算机在进行模糊逻辑处理时，首先从用户接口接收证据及其相应的模糊词，然后根据隶属度表确定每个条件模糊词的隶属度，进而进行推理得到结论。

由于一般的基于模糊逻辑的诊断方法采用了与基于规则的诊断方法类似的结构，因此它也具有基于规则的诊断方法的一些缺陷：

① 在推理时诊断时长和知识库内搜索量有关。一般情况下，知识库大，诊断时耗长。

② 模糊系统存在维护问题。

③ 模糊系统不具备学习能力，容易发生漏诊或误诊。

④ 用隶属函数表示模糊语言变量，两者之间的转换是一个难题。

1）故障定位的探测选择概述

当前一阶段故障检测完成后，我们会对探测结果进行分析，如检测到故障存在，那么就会进行故障定位阶段的探测选择，目的是定位故障的根源。为了达到这个目的，需要发

送合适的探测来获取更多的信息。

首先，我们对故障检测的探测结果进行分析。若探测成功，我们就认为成功探测经过的所有节点均为正常节点，并将这些节点加入正常节点集合N_{nn}（Normal Node），若有节点之前被判定为可疑节点，将其从可疑节点集合中删除；若探测失败，则失败探测路径上所有之前未被判定为正常节点的节点均为可疑节点，并加入可疑节点集合N_{sn}（Suspicious Node）；若一条失败探测所经过的所有节点中，仅有一个节点为可疑节点，其他节点都被某些成功探测经过，那么该可疑节点即为故障节点，并被加入故障节点集合N_{fn}（Fault Node）。

然后，通过对故障检测阶段探测返回结果的分析，可以得出正常节点集合、可疑节点集合以及故障节点集合。而可疑节点集合作为状态不确定的节点集合，将成为故障定位阶段的探测的目标。目前故障定位阶段的探测选择方法有两大类：预先选择探测方式和交互式选择探测方式。前者一次性选择出所有故障定位探测集合，发送到网络中并接收探测结果，预先选择的方式对网络施加固定的负荷，虽然这种方式计算过程比较简单，但是对所有的探测均以如此方式执行是极其低效的；交互式探测方式每次根据上一次探测的探测结果自适应地选择下一个探测，则可以有效减少所需执行探测的数量，从而得到更好的时效性和更低的额外网络负载，但计算过程往往异常复杂。这里选择交互式的探测思路来设计算法。

故障定位阶段的探测选择要求选择一个新的探测，该探测将要使得可疑节点集合中的节点数量尽量减少。这样选择的探测次数才会更少，才能够带来更少的额外网络负担。

对故障定位阶段的探测选择的评估指标如下：

① 探测次数。

② 判定故障节点的正确率。

2）故障定位的探测选择模型

故障定位阶段探测选择的建模也是探测依赖矩阵，和故障探测阶段的探测选择不同，本阶段的探测选择是从备选探测集合（未被作为探测的探测集合，在故障检测阶段表示除了故障检测集合以外的可用探测集合，在故障定位阶段表示除了故障检测集合和之前故障定位探测以外的可用探测集合）里面选取满足使可疑节点数尽量减少的探测。所以本阶段的探测必须覆盖可疑节点。

以下两种情况可用于减少可疑节点：

① 若只覆盖一个可疑节点的探测测试结果返回失败，则表明该可疑节点为故障节点；

② 若覆盖可疑节点的探测测试结果返回成功，则表明这些可疑节点为正常节点。

需要注意的是对于第2种情况，还要考虑由于把这些可疑节点从可疑节点集合删除，加入正常节点集合之后，之前测试集合中结果返回失败且覆盖多个可疑节点的探测可能现在只含有一个可疑节点了，需要对所有的然后失败的探测集合重新进行情况1的

判定。

3）故障定位的探测选择算法

（1）算法思路

故障定位阶段的探测选择有两种基本思路。

一是Max算法：每次选择一个经历N_{sn}中节点最多的探测。若这次探测成功，则将使得N_{sn}中的节点减少很多；反之，不能减少N_{sn}的节点。注意经历N_{sn}中所有节点的探测除外，因为该探测一定返回失败。

二是Min算法：每次选择经历N_{sn}中节点最少（至少为1个）的探测。若这次探测成功，则将使得N_{sn}中的节点减少至少1个；若探测失败，当且仅当它经历一个节点时，把该节点从N_{sn}中删除并加入N_{fn}。

一般来说，考虑到网络中出现故障的节点总是少数，相对来说即使经历N_{sn}中节点较多的探测成功的可能性也高于失败的可能性，选择Max算法会更好一些。但是，由于我们在探测站点的选择上只使用3个节点，会导致很多可疑节点是故障节点的后续节点，即这些可疑节点会伴随着故障节点一起出现，导致经历N_{sn}中节点较多的探测失败的可能性大大增加，所以我们选择Min算法。

（2）预处理

故障检测阶段测试结果分析：

① 把所有节点分别加入N_{nn}、N_{sn}、N_{fn}中。

② 记录所有返回结果失败的测试，把它们放到测试失败集合T_{ft}（Fault Test）中。

③ 将备用探测集合中经历故障节点的探测删除。

（3）算法流程

算法流程如图7-30所示。

步骤1：若$|N_{sn}|$为空或者备用探测集合中不包含经历可疑节点的探测则退出，否则将备用测试集合中所有经历N_{fn}的探测从备用测试集合中删除，然后转入步骤2。

步骤2：在备用探测集合选择经历N_{sn}中节点最少（至少为1个）的探测T_i，然后转入步骤3。

步骤3：若T_i探测结果返回成功，则将该探测经历N_{sn}中节点从N_{sn}中删除并加入N_{nn}，然后转入步骤4；若T_i探测结果返回失败，将该探测加入T_{ft}，若在结果返回失败且该探测中只有1个可疑节点，则将该可疑节点从N_{sn}中删除并加入N_{fn}中，然后转入步骤1。

步骤4：遍历T_{ft}，将其中满足有且仅有一个可疑节点的探测中的可疑节点从N_{sn}中删除并加入N_{fn}中，然后转入步骤1。

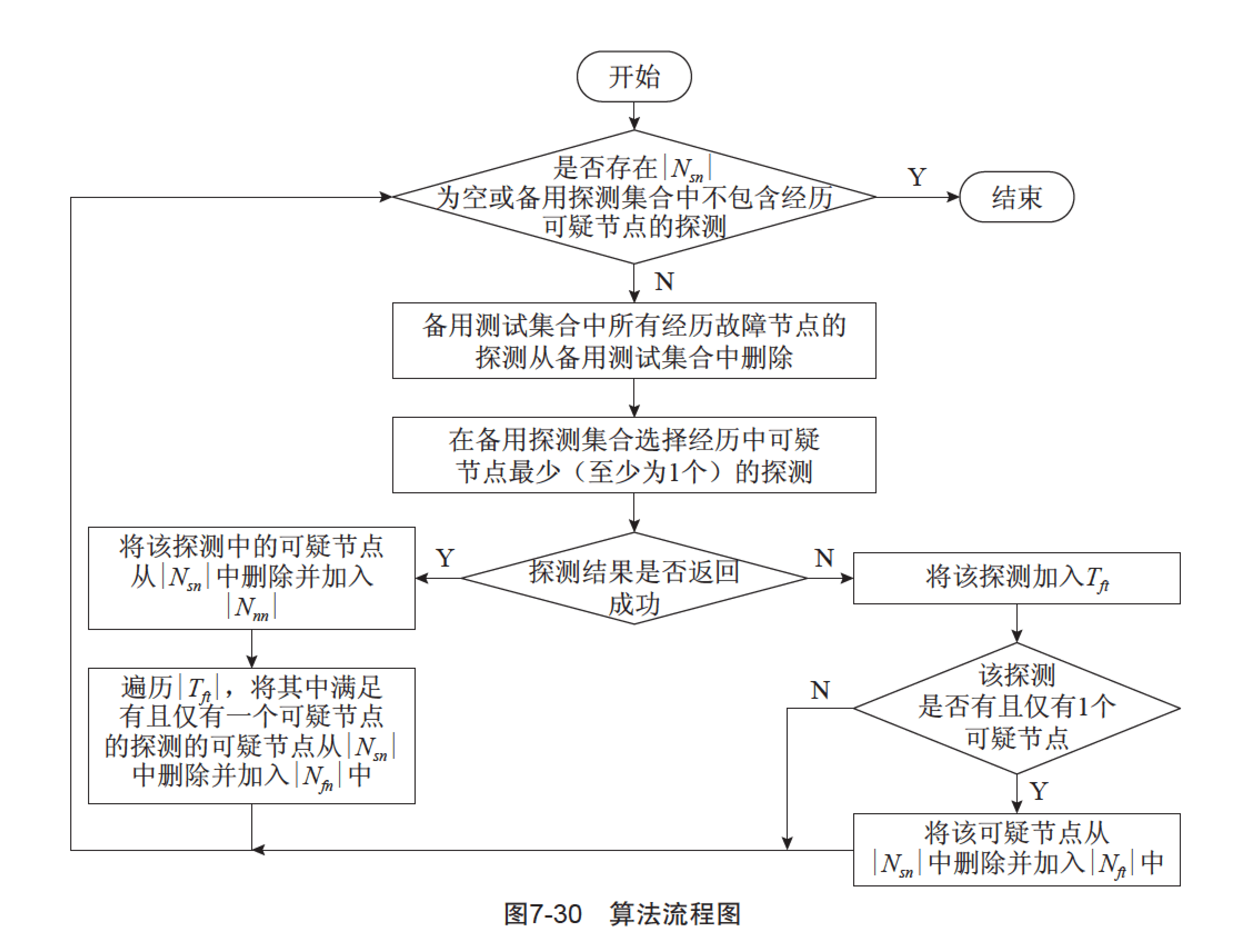


图7-30　算法流程图

7.9　运维支撑工具安全及权限管理策略

7.9.1　运维支撑工具安全及权限管理总体设计

运维支撑工具安全防护包括物理环境安全防护、网络安全防护、探针设备安全防护、主机安全防护、应用与数据安全防护等。

7.9.2　物理环境安全防护策略

物理环境分为室内物理环境和室外物理环境，应根据设备部署安装位置的不同，选择相应的防护措施。运维支撑工具作为室内系统，室内机房物理环境安全需满足对应信息系统等级的等级保护物理安全要求。

7.9.3 网络安全防护策略

运维支撑工具运行在终端通信接入网中，网络环境安全防护需遵循终端通信接入网的安全防护设计。网络环境具体包括网络中提供连接的路由、交换设备及安全防护体系建设所引入的安全设备、网络基础服务设施。

进行网络环境安全防护的目标是防范恶意人员通过网络对业务系统进行攻击，同时阻止恶意人员对网络设备发动的攻击。在安全事件发生前可以通过集中的日志审计、入侵检测时间分析等手段，以及对生产控制大区、配电终端、网络设备等安全状态的感知和监测，实现安全事件的提前预警，发现攻击意图。在安全事件发生后可以通过集中的事件审计系统及入侵检测系统进行事件追踪、事件源定位以发现恶意人员位置或及时制定相应的安全策略防止事件再次发生，实现事后审计，对恶意行为和操作的追查稽核、探测入侵、重建事件和系统条件，生成问题报告。

网络层基于“专网专用”的工作思路，采用独立的传输信道实现不同安全区业务的“物理隔离”（光纤通信采用独立纤芯、载波通信采用独立耦合装置、无线专网通信采用独立频段、无线公网采用独立接入装置）。

1. 有线通信

当采用EPON、工业以太网交换机、电力线载波等有线方式通信时，采用通信系统的鉴权、加密技术实施网络防护。

1）EPON

EPON接入方式的通信信道防护措施如图7-31所示。

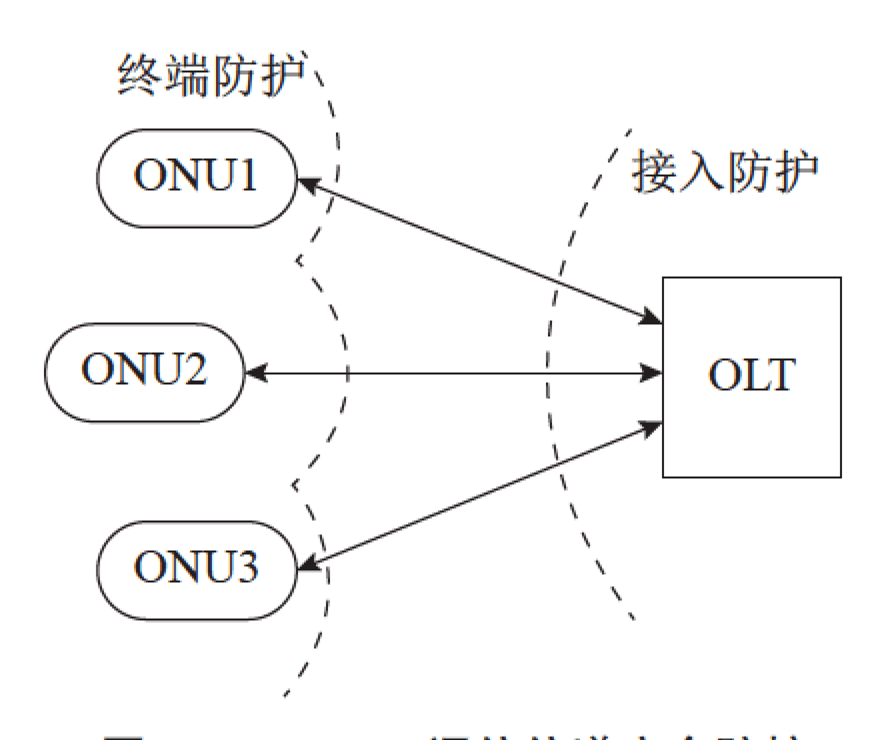


图7-31 EPON通信信道安全防护

① 在初始状态和数据通信两个阶段需要采用鉴权策略。在初始状态，ONU需要通过鉴权机制确认其身份，从而决定是否允许该ONU完成注册过程。在数据通信过程中，需进行用户鉴权，确认通信方是否为合法用户。

② 为保证合法用户信息的保密性，应采用加密技术对数据进行保护。应首选国家密

码管理局推荐的SM1算法，兼容AES算法和三重搅动加密算法，从而进一步增强接入层设备间的数据传输安全性。每个逻辑链路连接标识应有独立的密钥。

③ 将不同的ONU加入不同的VLAN或采用端口隔离特征，实现报文之间的逻辑隔离。

2）工业以太网

工业以太网通信安全主要包括客户端接入安全、多播安全以及交换机自身抗攻击性能等。

① 客户端接入安全。常用的方案包括限制MAC地址数量，在交换机的地址学习表中静态绑定设备的MAC地址；采用IEEE 802.1x认证方式实现终端的安全接入等。

② 多播安全。多播访问控制的目的是对终端是否合法接受多播报文进行配置，可将多播泛洪抑制在特定的范围内。交换机多播过滤可通过静态多播配置和动态多播分配两种方式实现，静态多播即将多播MAC添加到交换机二层地址转发表中；动态多播分配则通过协议的方式实现，目前常用的有GMRP和IGMP Snooping。

③ 防ARP、ICMP攻击。为防止ARP 和Internet 控制报文协议（Internet Control Message Protocol，ICMP）攻击，要求交换机支持ARP防扫描、ARP防欺骗以及ICMP 防攻击特性。

④ 逻辑隔离和加密。支持基于端口或标记的VLAN划分，实现不同类型业务的逻辑隔离；采用IPSec隧道等方式对传输信息进行加密处理等。

3）电力线载波

电力线载波以电力线为通信媒介，通信通道“开放”，在安全接入方面需重点加强接入认证、对信息传输要采取加密措施。

① MAC层认证。配电网中的根节点负责所管理的所有新节点的注册请求服务，成功注册的新节点才能获得有效的通信ID。认证消息的加密解密通过AES等算法实现。

② IEEE 802.1x服务认证。认证系统采用IEEE 802.1x标准，其中扩展认证协议采用EAP，认证服务器采用 RADIUS 服务器，密钥管理采用四步握手协商机制。

③ 白名单管理机制。白名单用于维护网络中有效节点，并周期性更新白名单，对于存在于白名单内的节点采取四次握手方式进行EAP认证，否则将直接拒绝该节点入网申请。

④ 信息加密。对传输的信息通过DES、AES等算法进行加密。

2. 无线公网

无线公网接入模式借助电信运营商的无线公共网络传输电力数据。电力公司应对运营商提出安全措施要求，包括：

① 采用APN+VPN或VPDN技术实现无线虚拟专有通道。

② 通过认证服务器对接入终端进行身份认证和地址分配。

③ 在主站系统和公共网络采用有线专线+GRE等手段。

④ 运营商与电力公司传输数据时，通过安全接入平台接入电力公司内网。

图7-32所示为增强安全组网架构示意图。

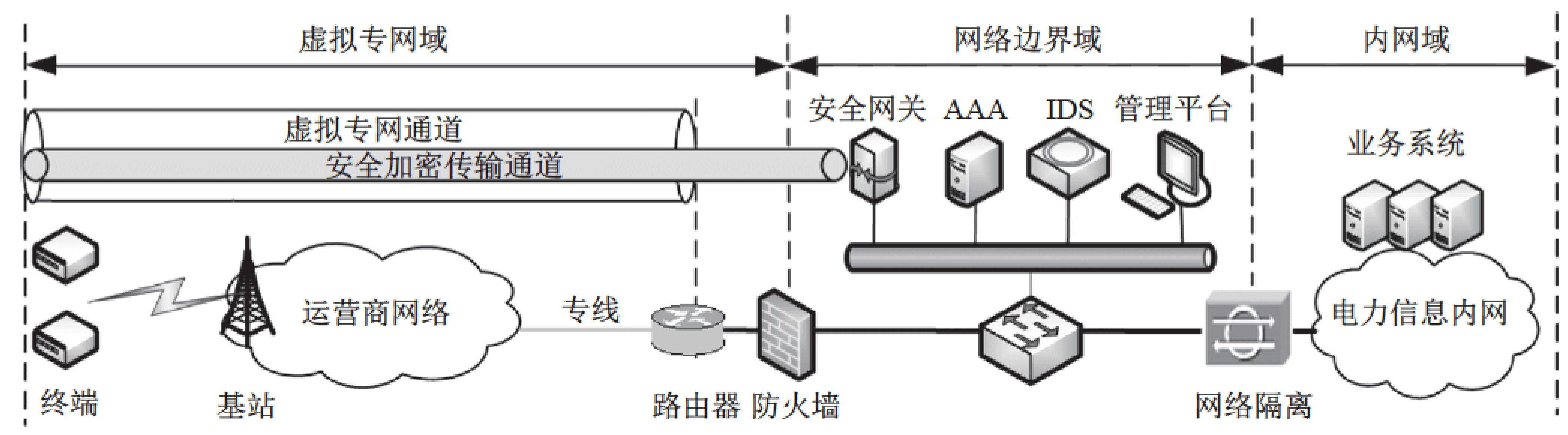


图7-32 增强安全组网架构示意图

如图7-32所示，终端使用专用APN接入运营商2G/3G/4G无线网络，运营商负责对终端SIM/UIM卡信息进行认证鉴权，禁止非法SIM/UIM卡接入。

采用AAA系统对接入增强安全无线虚拟专网的用户进行认证、授权、记账，禁止非法用户接入，同时对用户授权、记账。

根据需要可进行SIM/UIM卡+用户+终端硬件的绑定，实现SIM/UIM卡、用户、终端硬件的一一对应。

采用L2TP、MPLS-VPN等VPN技术在运营商网络中建立虚拟专网传输隧道。

在网络边界部署安全网关，在终端与安全网关之间建立安全加密隧道（VPN）传输业务数据。终端发起隧道连接时应对终端VPN用户进行双因素认证。

网络边界应部署防火墙、入侵检测、网络隔离等设备进行网络安全防护，应实现完善的访问控制、DDoS攻击防护、入侵检测及网络隔离防护。

建立管理平台实现告警管理、性能管理、流量管理、资源管理、状态管理、位置信息管理、统计报表、系统管理、账单管理、日志审计等功能。

3. 无线专网

当采用专用无线网络时，分别针对无线接入层和非接入层采用相应的信息安全措施。无线接入层指从无线通信终端到基站之间的空口传输链路；非接入层指从无线通信终端到无线核心网的链路。无线接入层和非接入层的安全措施应分别独立运作，安全防护体系的总体结构如图7-33所示。

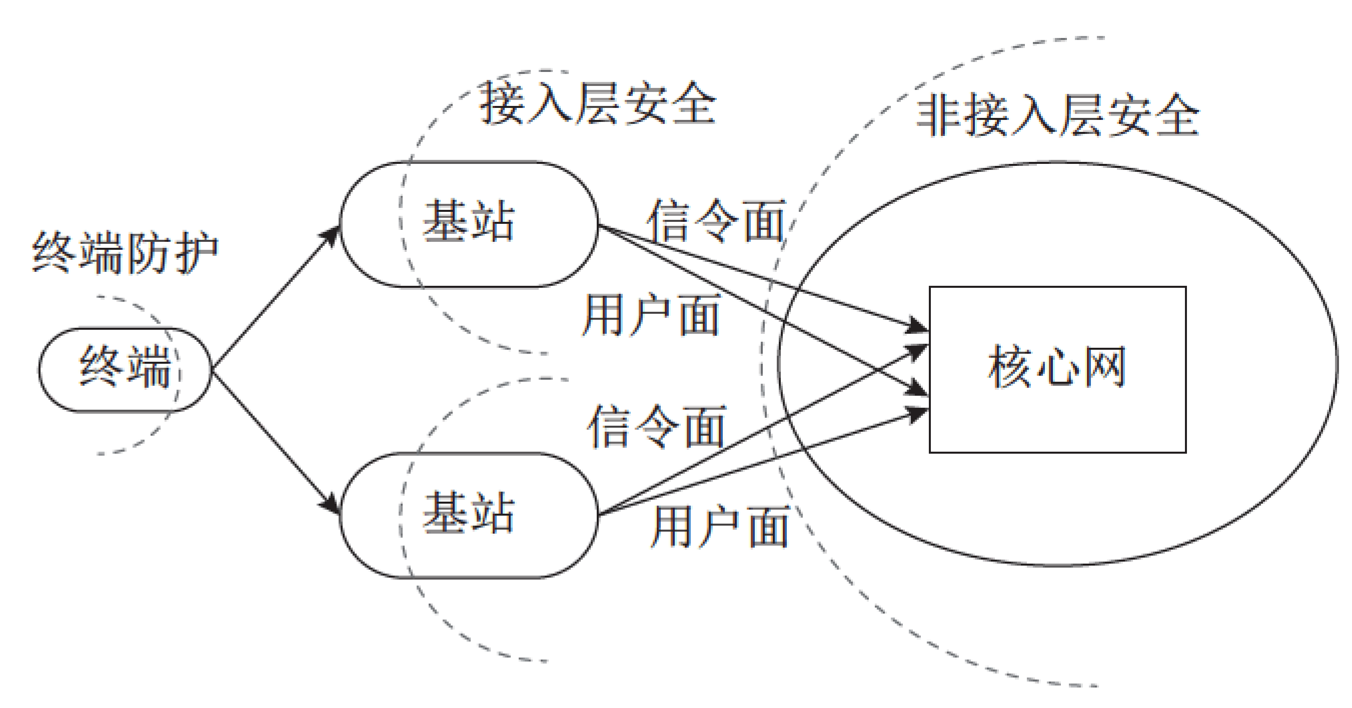


图7-33 无线专网安全防护

无线接入层和非接入层所采用的具体安全措施均包含双向鉴权认证、安全性激活、信令和数据的机密性及完整性保护。无线接入层和非接入层的安全措施类似，但应采用不同的密钥以保证各自独立运作，如图7-34所示。

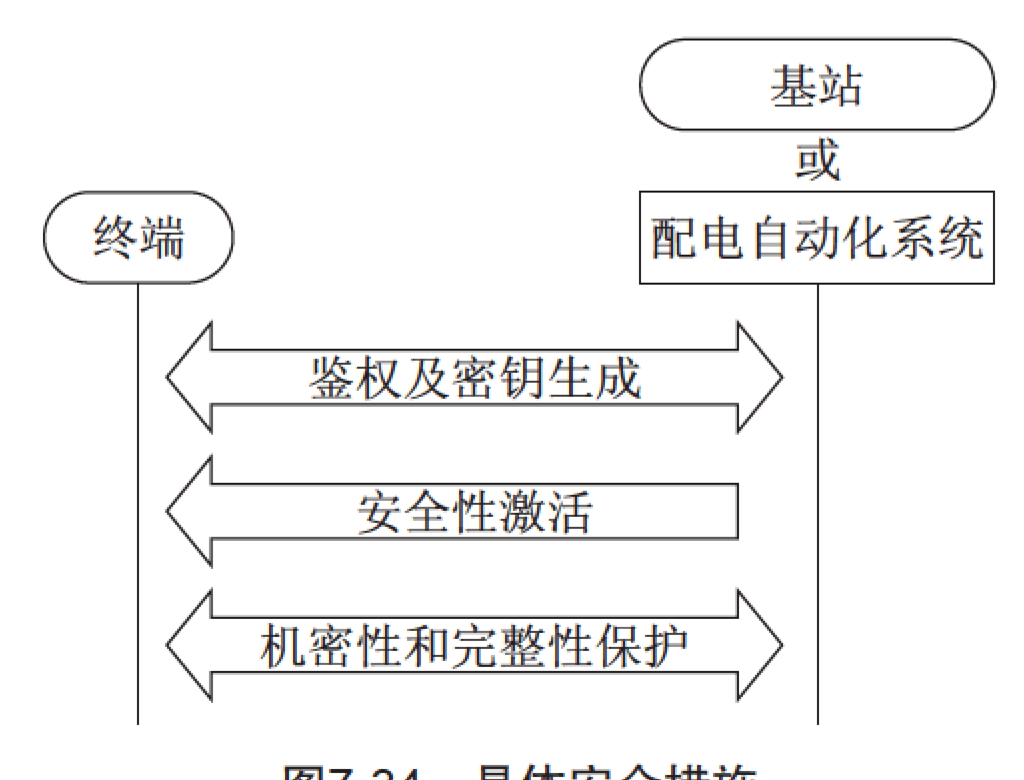


图7-34　具体安全措施

① 鉴权与密钥协商过程：应实现通信两端的双向鉴权，并保障两端密钥达成一致。通信双方在共同持有根密钥的前提下，通过协商过程相互认证对方的合法身份，并计算出后续安全措施所用的密钥。密钥生成算法的输入应包含帧序号或时间戳等信息以确保密钥的时间有效性，防止重放攻击。

② 安全性激活过程：验证通信双方安全模式和加密算法的统一。通信双方通过校验安全模式命令的完整性确认双方具备相同的安全模式，协商所要采用的加密算法及完整性校验算法。非接入层的激活应先于无线接入层。

③ 信令加密和数据加密过程：应实现通信信令和数据的机密性保护。使用密钥协商过程中生成的加密密钥对信令和数据进行加密传输，保护数据的机密性。所采用的加密算法可选择SM1、ZUC或AES，由安全性激活过程确认。加密信令和数据应使用不同的加密密钥。

④ 信令和数据的完整性校验：应实现通信信令和数据的完整性保护。使用密钥协商过程中生成的完整性密钥进行数据完整性校验，保护数据完整性。具体校验方式可选择CRC或MAC，由安全性激活过程确认。信令和数据的校验应使用不同的完整性密钥。

当采用无线专网承载不同安全区业务时，应采用不同频段，在无线终端接入侧每类业务分别接入不同的CPE终端，实现无线终端接入的物理隔离，如图7-35所示。

无线空中传输物理隔离：为不同类型的业务划分不同的无线频段，通过频谱间的保护间隔，确保无线接口传输信道之间的物理隔离。

基站侧物理隔离：基站根据VPN或APN划分，将从射频端收到的数据包处理后通过不同的上联端口发送到承载相应安全区业务的核心网设备。在基站内部，不同频段接收的业务数据在独立的业务板进行处理，保证基站内的多业务物理隔离。

VPN隔离：骨干传输网采用VPN隔离（利用高安全可靠性的IPSec协议封装），为不同类型业务传输划分独立的逻辑通道。

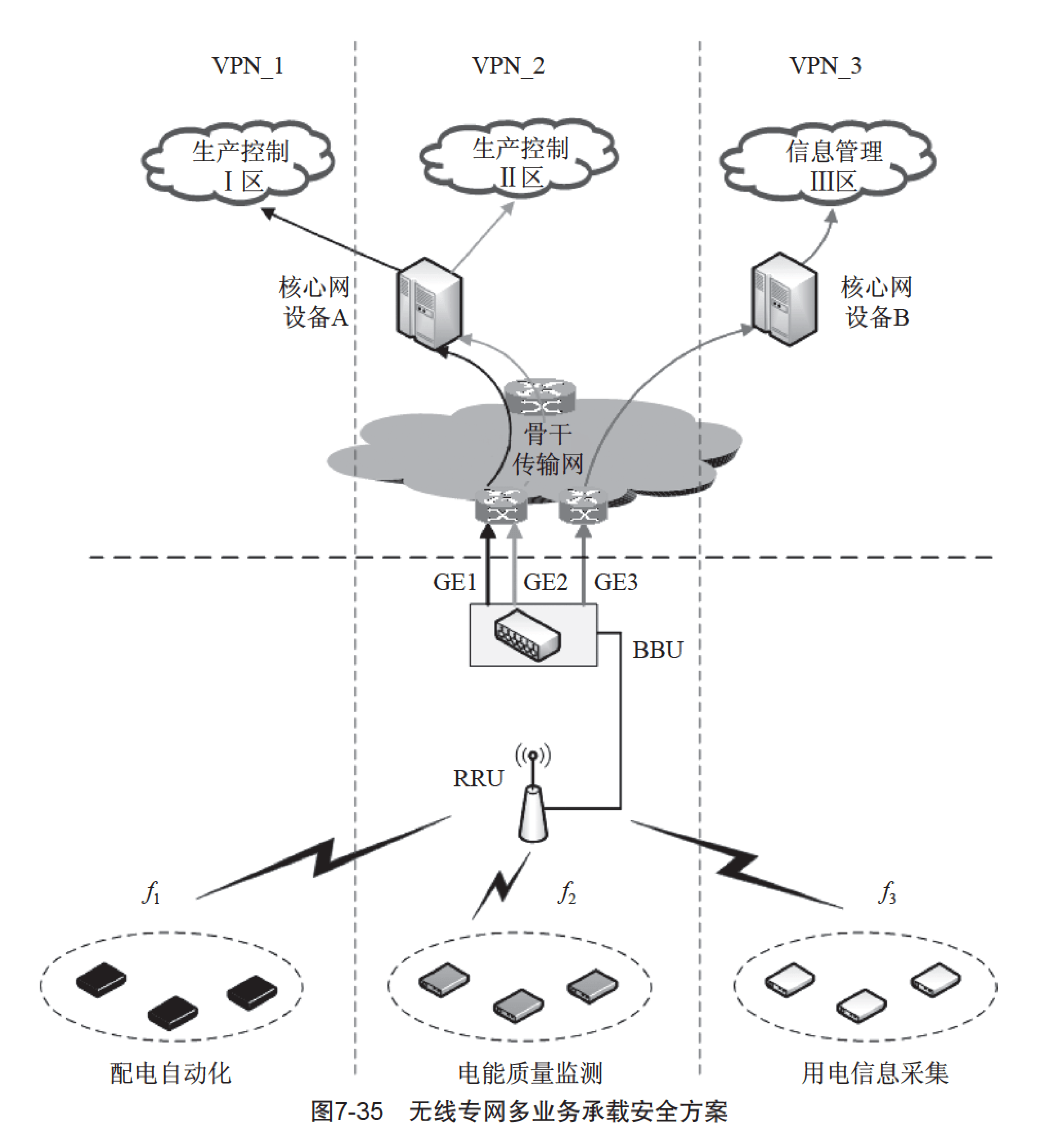


图7-35 无线专网多业务承载安全方案

核心网设备物理隔离：Ⅰ、Ⅱ区业务接入核心网设备A，Ⅲ区业务接入核心网设备B，每个核心网设备为各类业务指定不同的接入端口和上联端口，实现同一设备不同业务的隔离。

通过上述技术手段，实现从终端到主站整个无线通信网络的多业务安全隔离。

7.9.4 探针设备安全防护策略

对于运维支撑工具的探针设备和服务器设备，采用访问控制、安全加固、监控审计、身份鉴别、备份恢复、设备弱点扫描、安全事件审计、配置文件备份等方面的网络设备安全防护。设备安全防护措施如表7-17所示。

表7-17　设备安全控制措施

安全控制措施	控制措施实现方式
安全接入控制	对于探针设备采用802.1X等网络准入控制手段实行准入控制，同时采用IP与MAC地址绑定等手段以防止网络地址欺骗
设备安全管理	实现设备安全管理，主要包括以下安全控制措施： 本地或远程进行设备管理时必须进行身份认证； 制定设备管理策略，包括限定管理IP地址、制定登录超时及账号锁定策略； 采用较为安全的SSH、HTTPS进行远程管理； 对基于SNMP协议进行网络监控及管理，采用SNMP V3版本，Community不应使用Public、Private等默认字段
设备安全加固	对于网络及安全设备的加固主要包括两部分： 依据设备厂商或专业安全机构提供的安全配置列表进行网络设备安全加固； 及时升级设备系统或安装安全更新补丁
安全弱点扫描	使用特征代码库更新后的专用弱点扫描系统在非业务高峰期对网络及安全设备进行扫描，并根据扫描出的弱点及时处理
配置文件备份	每个月或当配置发生变更时进行配置文件备份
设备安全审计	建立集中审计系统对主站系统安全域中网络及安全设备日志进行集中收集存储； 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； 定期对所收集的日志进行事件审计分析，也可采用自动审计系统或事件分析系统进行安全事件审计分析

7.9.5　主机安全防护策略

服务器主机是所有应用的基石，服务器一旦出现故障，所有信息化服务将停止。系统主机安全主要从以下方面考虑。

1. 国产安全操作系统

运维辅助工具运行在国产安全操作系统之上，国产操作系统满足国家等级保护要求中具有四级防护能力的B级操作系统。

2. 主机冗余

建立双主机系统，利用操作系统、数据库系统或其他第三方系统，实现服务器主机、应用服务双机冗余备份，双网链路接入网络交换设备，从物理底层避免单点故障；视应用系统软件特性，对应用系统进行集群建设，使应用系统在物理和应用两个层面上均实现双机甚至多机系统，全面降低单点故障对整个信息系统的影响。

3. 主机加固系统

服务器主机系统可考虑增加主机加固软件系统。主机加固系统基于操作系统的内核开

发，即使操作系统存在各种漏洞，只要装上此类产品后，不用打补丁，亦可进行防范。还可以增加HIPS（HostIPS）主机入侵防护系统，以保障数据的访问安全。

4. 操作系统安全补丁

操作系统及应用系统及时进行安全补丁安装，可以有效减少受攻击和危害的可能性。由于电力系统内外网隔离，因此可以采用在内网建立安全补丁分发服务器作为二次分发的方式实现，做到及时升级；对于部分升级敏感的服务和应用，可以采用在服务器网络前端部署IPS的方式，在IPS上注入数字疫苗，实现虚拟补丁功能，最大限度地保障服务器系统安全。

5. 防病毒软件

采用统一管理的网络化防毒软件，实现原厂病毒数据库自动拖拽升级，强制分发等方式，保持服务器主机系统防病毒系统处于最新状态，辅以自定义安全策略，实现对某些特殊安全威胁的控制。

7.9.6 应用与数据安全防护和权限管理策略

1. 用户标识

系统保证每个用户只拥有唯一的用户ID标识和唯一的密码标识，防止因为用户标识不唯一的而导致某个用户访问到非授权信息。

系统对于关键信息，如实时数据库、关系数据库、FTP服务器的用户名、密码等关键信息采用加密方式存储，从而保证系统关键信息不泄露。用户在访问应用系统的时候，应用系统通过统一授权系统的接口查询、验证此用户是否有权使用该功能，根据统一授权管理和统一的用户身份认证管理系统返回的结果进行相应处理。

用户认证系统还可方便地与具有更强安全性的CA 认证系统集成，兼容第三方的CA认证系统，支持用户认证、数字签名、时间戳、数据加解密等功能。

2. 用户鉴别

系统需提供最基本的用户名+口令的身份鉴别机制。系统不能使用默认密码、初始密码或匿名用户登录系统。如果是新建立的系统用户，将在用户初次登录时强制用户修改登录密码。

3. 鉴别失败

系统配置文件中设置有登录尝试失败次数（通常是 3~5次），确保超出允许的尝试次

数之后，便锁定账户。为了避免真正的用户因账户被锁定而致电支持人员的麻烦，可以仅临时性暂挂账户活动，并在特定时间段之后启用账户。账户锁定大约 10min，通常便足以阻止蛮力攻击。

当试图利用不正确的凭证来登录时，如用户输入无效的用户名和无效的密码时，应用程序会分别生成不同的错误消息。利用该行为，攻击者便可以通过反复试验（蛮力攻击技术）来发现应用程序的有效用户名，再继续尝试发现相关联的密码。这样会得到有效用户名和密码的枚举，攻击者便可以用来访问账户。

针对登录尝试的攻击，可以使用相同的报错信息，例如都是提示“输入的用户名或者密码错误！”。

4. 密码规范

系统管理模块将对用户的密码安全性、规范性进行要求。登录密码必须有长度限制、复杂度限制，以及最长使用时间限制。密码的安全强度可在配置文件中配置。

5. 多重鉴别机制

系统提供多种组合身份鉴别机制，如用户名密码、验证码、数字证书、动态令牌等身份鉴别机制。

6. 权限控制功能

系统提供严格的访问控制和权限控制能力。系统的全局安全拦截器将对所有的系统功能模块进行严格安全检查。系统基本的用户角色分为系统管理员、审计管理员、审核管理员、业务操作员。这四类用户操作权限为互斥关系，不同类型的操作权限不可被同一个用户拥有，防止出现安全操作事故。

7. 权限控制策略

系统中的用户保证只被授予完成各自承担任务所需的最小权限，不同角色之间需具有相互制约的关系。系统管理员、审计管理员、审核管理员之间的操作权限各自独立分开。

对某些重要的操作，如信息发布（审核），除了各个栏目可以设置特定的角色、用户外，还可设置是否需要控制操作客户端机器的IP地址。当指定某操作需要进行IP地址绑定时，操作前先判断操作请求客户端IP是否位于ACL（控制访问列表）中，只有属于ACL中的IP地址，才进行角色、用户等权限检测，否则拒绝操作。

8. 未登录授权绕过

每个成功登录的用户，将在服务端维持一个全局唯一的会话标识。只有包含合法会话标识的HTTP请求，才被认为是合法请求并允许进入系统。所有未经成功用户身份鉴别

的非法请求将不能进入系统。防止用户采用正常登录过程，从系统内部复制系统关键操作URL，然后在不登录系统的情况下直接访问系统内部功能或资源。

① 有效控制栏目（菜单）的权限。系统可以对任意栏目（菜单）的权限进行控制，只有有特定权限的角色或用户才能使用该栏目（菜单），无权限的用户无法使用该栏目（包括该栏目下的子栏目）；而且，系统在业务逻辑的入口处还会根据五级业务授权的结果再做统一的权限判断，这样即使用户使用直接在浏览器输入地址的方式也无法访问其业务权限之外的内容。

② 五级业务授权管理模式。系统支持五级业务授权管理模式，即应用级授权、类型级授权、对象实体级授权、对象属性级授权和工作流授权，每级授权都能进一步细分到具体功能或操作，从而实现多粒度权限划分和管理。

③ 基于角色的权限管理策略。系统支持基于角色的权限管理模型，通过角色建立起用户和资源间的联系，使得权限转移和代理可以被有效控制。

9. 登录后授权绕过

系统攻击者可以使用普通用户登录系统后，构造系统管理员的管理页面URL进行访问，从而达到获取系统敏感信息或对系统进行破坏的目的。

为了防止有登录后可被授权绕过的漏洞，需要使用Web过滤器对系统的每个URL都进行验证。其次，系统管理的页面仅允许系统管理员访问。

10. 审计数据产生

为防止赋权的用户不正当地使用系统，任何人的任何基本业务操作将被记录在系统的审计日志文件中。系统管理员通过日志的审计工具就可以对日志内容进行查询和审核，从而对用户的行为进行监督，及时发现违规行为，为业务工作的有序开展提供依据。这种审计记录是基于用户身份的，它可以准确地记录用户对资源访问的详细情况，为追查责任提供依据。

DICP系统根据三权分立的思想，将系统用户分为系统管理员、审计管理员、审核管理员和系统操作员。

审计管理员可以对系统的操作日志，在线用户、系统权限分配日志进行审计。

在进行用户登录、密码修改、权限管理等操作时，系统需将操作信息写入审计日志表中，审计信息存入审计日志表中，包含访问者的IP、当前用户、访问时间等信息。

11. 审计查阅

审计日志可采用Web页面中的数据列表或统计图表等方式展示，并提供按照审计日志相关关键字进行排序、查询、过滤的功能。对于可疑操作的审计日志采用高亮方式显示。

审计日志按照操作类型分为身份鉴别、权限变更、系统配置、业务操作等类型的审计

日志，可按照审计日志不同类型进行分类查看。

12. 审计事件存储

审计日志可保存在数据库表中，并可以导出为Excel表下载查看并保存。

13. 数据存储完整性

对于系统的关键信息，为了防止被非法用户篡改，需在系统中加密存储。同时，为了保证加密数据的完整性，需在加密内容中增加额外的数据完整性校验码，在对数据解密完成后，重新进行校验码计算，并与之前的校验码进行比较，如果一致则说明数据完整性没有被破坏。

14. 数据传输完整性

通过网络传输数据，需要保证数据的完整性、保密性，以及能够对数据的发送者进行身份验证。这些都需要通过一些加密算法实现，数据的加密方式有：

① 对称加密：加密和解密使用同一个密钥。其特点是保证了数据的保密性，局限是无法解决密钥交换问题。常用的算法有DES、3DES和AES。

② 公钥加密：生成一个密钥对（私钥和公钥），加密时用私钥加密，解密时用公钥解密。其特点是解决了密钥交换问题，局限是对大的数据加密速度慢。

③ 单向加密：提取数据的特征码。其特点是定长输出，不可逆，可检验数据的完整性，局限是无法保证数据的保密性。常用算法有MD5、SHA1和CRC-32。

三种加密方法各有优缺点，在实际应用中，数据从发送方到达接收方，通常是这样应用的：

① 首先对要发送的数据做单向加密，获取数据的特征码。

② 对特征码用发送方的私钥进行加密生成S1。

③ 然后对S1和数据进行对称加密生成S2。

④ 最后将S2和对称加密的密码使用接收方的公钥进行加密。

这样一来数据在传输过程中的完整性、保密性以及对发送方身份的验证都能得到保障。

当数据到达接收方时，接收方先用自己的私钥对接收到的数据进行解密，得到密码和加密的数据；使用密码对加密数据解密，得到加密的特征码和数据；用发送方的公钥解密特征码，如果能解密，则说明该数据是由发送方所发；反之则不是，这便实现了身份验证；最后计算数据的特征码和解密出来的特征码并做对比，如果一样，则表示该数据没有被修改，反之则表示数据被修改过了。

15. 数据存储保密性

保护与加密敏感数据已经成为网络应用的最重要的组成部分。简单不加密的敏感数据是

非常普遍存在的。不加密的应用程序设计不当往往含有密码，也可能程序使用了不恰当的密码或密码在发生强烈的严重错误时使用。这些缺陷可以导致违反披露敏感数据的遵守原则。

解决数据存储保密性的解决办法有：

- 识别所有的敏感数据；
- 识别这些数据存放的所有位置；
- 使用加密手段来应对威胁；
- 使用一定的机制来进行保护；
- 文件加密；
- 数据库加密；
- 数据元素加密；
- 正确使用以上这些机制；
- 合理生成、分发和保护密钥；
- 确保使用准的强算法；
- 确保所有的证书、密钥和密码都得到安全的存放；
- 有一个安全的密钥分发和应急处理方案。

16. 数据传输保密性

对于不加密的应用程序的网络信息传输，需要保护敏感的通信；加密（通常SSL）的必须用于所有身份验证的连接，特别是通过Internet访问的网页，以及后端的连接，否则应用程序将暴露身份验证或会话令牌。

为了防止系统的数据在传输过程中被第三方嗅探监听或篡改，调度管理系统采用了基于数字证书的双向认证方式对传输内容进行加密。保证传输内容在网络中采用SSL方式进行加密传输。同时，基于数字证书的双向认证方式，保证了只有拥有系统认证服务器办法的私钥用户才可以访问系统。

17. 跨站脚本攻击

跨站脚本是最普遍的Web应用安全漏洞。当应用程序在发送给浏览器的页面中包含用户提供的数据，但没有经过适当验证或转义那些非法内容时，就导致了跨站脚本漏洞。

攻击者能在受害者浏览器中执行脚本以劫持用户会话、迫害网站、插入恶意内容、重定向用户、使用恶意软件劫持用户浏览器等。

在调度管理系统中，通过全局拦截器根据特征对跨站脚本进行拦截并进行转义或过滤，从而避免了系统遭到跨站脚本的攻击。

18. 敏感信息泄露

应用程序常常产生错误信息并显示给使用者。很多时候，这些错误信息对于攻击是非

常有用的，因为它们揭示了可利用的实施细则或有用的开发信息漏洞。

敏感信息泄露的主要危害有：

- 泄露太多的细节（如错误堆栈跟踪信息、SQL语句等）。
- 登录失败后，通知用户是否用户ID或密码出错——登录失败可能是由于ID或密码错误造成的。这为一个对关键资产发动蛮力攻击的攻击者提供了重要信息。

针对敏感信息泄露的问题，可以通过自定义Web应用程序的错误页面，屏蔽掉敏感信息。对于系统的错误信息，使用错误代码而不是错误的详细信息，从而使攻击者不能获取更多的系统信息。

19. SQL注入漏洞

SQL注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意SQL命令的目的。

SQL注入能导致数据丢失或数据破坏、缺乏可审计性或是拒绝服务。注入漏洞有时甚至能导致主机被完全接管。

SQL注入是由于应用程序缺少对输入进行安全性检查所引起的，非法攻击者把一些包含SQL语句的数据发送给解释器，解释器会把收到的数据转换成SQL语句来执行。

调度管理系统中，使用参数化查询、存储过程查询，对查询SQL参数进行安全过滤等方法来解决SQL注入攻击。

20. 数据有效性验证

数据的合法性鉴别主要包含了客户端和服务器端的鉴别。在客户端中当提交表单的时候对每个控件做校验，校验的种类包含了非空、字段长度、正则校验。

在服务器端则包含了两方面，其一是在表单提交数据的时候，依次对提交的数据做合法性校验；其二是利用Struts的validation框架做校验。

21. 文件上传漏洞

文件上传漏洞是指攻击者利用系统的文件上传功能上传非法代码并执行的攻击方式。比较常见的如上传.jsp文件到Web目录，并执行非法操作。解决办法是，检查客户上传文件的文件类型，不允许可执行的代码文件被上传到服务器，其次，上传文件不要保存在Web目录中，防止被直接在Web目录执行。

22. 文件下载漏洞

文件下载漏洞是指攻击者对正常的文件下载URL构造特殊的参数，下载非授权的系统敏感文件。

可以在程序中对下载的文件路径进行检查，限制在特定的Web目录下。其次，为Web

应用建立专门的用户，并赋予必要的系统权限，避免越权访问系统信息。

23. 会话超时

用户登录到系统中，将会在服务端内存中维持一个会话标识。每个会话有一个超时时间，如果在超过超时时间设置的时间段内，用户没有任何操作，则认为该会话超时。超时的用户会话将在服务端内存中销毁。客户端使用超时的用户会话将不能再次访问系统。避免非法用户在登录过系统的机器上直接输入URL非法进入系统。

24. 并发会话限制

系统可设置并发会话限制，如系统最大登录用户数不能超过某个阈值，同一个用户不能在系统中登录多次。防止非法攻击者采用脚本或自动化工具对系统发起登录请求导致系统瘫痪。

25. 溢出测试

攻击者利用超出缓冲区大小的请求和构造的二进制代码让服务器执行溢出堆栈中的恶意指令。系统的用户输入界面中需对合法输入的长度做限制和合法性校验，防止非法攻击者输入超长内容的数据对系统产生溢出错误。其次，在应用服务器前端可架设Apache或Nginx等代理服务器，并对HTTP的URL长度、Cookie大小、HTTP Body大小进行检查，避免系统发生溢出漏洞。

26. 端口扫描

在操作系统、防火墙中只开发必要的系统使用端口，不允许将非系统必要使用的端口开放给用户或外部攻击者。可使用防火墙或系统的iptables服务屏蔽不必要的端口。

27. 敏感信息探测

非法攻击者通过对Web服务器返回信息标头进行分析可获取到服务器的类型和版本号信息。因此需要将返回信息进行过滤，使攻击者无法获取Web服务器的版本和类型。

28. 中间人攻击

中间人攻击（Man-in-the-MiddleAttack，MITM）。中间人攻击很早就成为黑客常用的一种攻击手段。

中间人攻击会造成信息泄露和信息篡改安全风险，创建的中间人攻击有DNS劫持、会话劫持等攻击方式。

对于DNS欺骗，要记得检查本机的HOSTS文件，以免被攻击者加入恶意站点；其次要确认自己使用的DNS服务器是调度管理系统合法提供的。

至于局域网内各种各样的会话劫持（局域网内的代理除外），因为它们都要结合嗅探以及欺骗技术在内的攻击手段，必须依靠ARP和MAC做基础，所以网管应该使用交换式网络（通过交换机传输）代替共享式网络（通过集线器传输），这可以降低被窃听的机率，还可以使用静态ARP、捆绑MAC+IP等方法来限制欺骗，以及采用认证方式的连接等。

7.10　运维支撑工具接入访问控制技术方案

终端通信接入网是电力骨干通信网络的延伸，提供配用电业务终端与电力骨干通信网络的连接，具有业务承载和信息传送功能。在研究现有终端通信接入网访问控制方案的基础上，针对现有网络访问控制现状提出了运维支撑工具的访问控制设计方案，使之适应终端通信接入网生产控制大区“安全分区、网络专用、横向隔离、纵向认证”，管理信息大区“分区分域、安全接入、动态感知、全面防护”的总体安全策略。

7.10.1　终端通信接入网访问控制机制

1. 信息安全政策

信息安全政策将基于计算机及网络技术的智能设备以及通信数据网络等纳入电力监控系统的范畴；增加了落实国家信息安全等级保护制度和政策要求；对电力监控系统设备选型及配置做了进一步的明确要求，对电力监控系统实施方案的审核和验收进行了明确规定。

管理信息大区的安全防护在继承完善SG186工程以“双网双机、分区分域、等级防护、多层防御”为核心的等级保护纵深防御策略的基础上，部署先进适用的信息安全核心装备，并进一步遵从“双网双机、分区分域、安全接入、动态感知、精益管理、全面防护”的主动防御策略，进行智能电网信息安全防护。

深化信息安全主动防御体系，优化安全顶层设计；建立安全情报收集、研判和安全审查机制，构建精益高效全生命周期安全管理内控体系；深化全景可视预警监测，强化智能移动终端、无线网络安全，健全敏感数据防泄露措施，实现信息安全基础设施协同联动；深化云计算、物联网、大数据、移动互联新技术安全，打造智能可控的新一代安全技术防护体系，实现信息安全对智能电网业务和新技术应用的推动引领。

在信息安全顶层设计技术防护内容中提出：终端主机安全可控、网络边界安全可信、应用数据安全可管、监控预警分析全景可视、基础设施防护高效协同的内涵。

该设计明确了适应智能电网业务互联互通的需求，推进安全可信网络边界防护设备技术研究及研发，开展信息外网安全交互平台、信息内网安全接入平台、信息网络隔离装置升级改造；强化了通信传输网、接入网安全分区、物理隔离措施，提升通信网络边界安全防护水平；优化了路由器、防火墙、入侵检测/防御等通用边界安全设备的部署结构和配置策略。

2. 生产控制大区接入访问控制

生产控制区分为控制区和非控制区，控制区是电力生产的重要环节，直接实现对电力一次系统的实时监控，是安全防护的重点与核心；非控制区是电力生产的必要环节，在线运行但不具备控制功能，与控制区中的业务系统或其功能模块交互紧密。生产控制大区业务包括配电自动化、负荷控制、电能量采集、故障指示器监测、电动汽车充换电及分布式电源业务等。生产控制大区的边界主要指配电自动化终端、能量管理终端、负荷管理终端、电力数据采集和监控类终端通过接入网接入到业务系统的生产控制大区的边界、控制区和非控制区边界、生产控制大区和管理信息大区边界。具体的安全防护要求包括：

1）访问控制

生产控制大区与管理信息大区业务系统通信时应采用正反向隔离装置。

控制区业务系统与非控制区业务系统通信时应采用逻辑隔离防护措施。

当采用公网传输通道时，公网前置机应配置主站安全模块（安全网关、密码机、加密卡等），宜采用安全接入平台，至少包括安全接入网关和安全数据过滤系统等重要组件，完成对各种终端安全接入过程的全程控制；公网前置机必须采用电力专用的正反向隔离装置与业务系统进行隔离。

当采用专网传输通道时，专网前置机应配置主站安全模块，实现安全隔离、加密、认证功能。对于实时控制等重要业务，应通过纵向加密认证装置或加密认证网关接入。

应在边界防护设备上控制网络最大流量及并发连接数。

对于边界防护设备的策略违背行为应当采取安全审计措施，记录日志并定期分析处理。访问控制策略要严格到协议、地址和端口。

2）安全接入

应在主站侧部署加密装置进行安全认证，保证业务系统接入的可信性，禁止未授权的节点接入骨干网进行业务系统应用。

应对接入生产控制大区的业务终端身份进行鉴别和控制权限。

对于用户电脑或手机以Web方式访问骨干网时，应当进行身份认证，至少采用用户名/密码认证，并对密码长度、复杂度、生存周期等进行强制要求，制定用户登录错误锁定及会话超时断开等安全策略以保证终端接入安全。

3）入侵检测

应具备监测入侵行为的机制。

应采用入侵检测系统对流经边界的信息流进行入侵检测。入侵检测系统应当对主要的攻击行为进行检测，防止使用常用端口传输恶意信息，防止对服务器发动应用层攻击。

应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP地址、攻击类型、攻击目的、攻击时间，并在发生严重入侵事件时提供告警。

生产控制大区无线技术安全接入区。

生产控制大区中的业务系统，如果纵向联接使用无线技术，电力企业数据网或公用数据网使用VPN方式，应当设立“安全接入区”，安全接入区与控制大区中其他部分的连接处必须设置经国家制定部门检测认证的电力专用横向单向安全隔离装置，如图7-36所示。

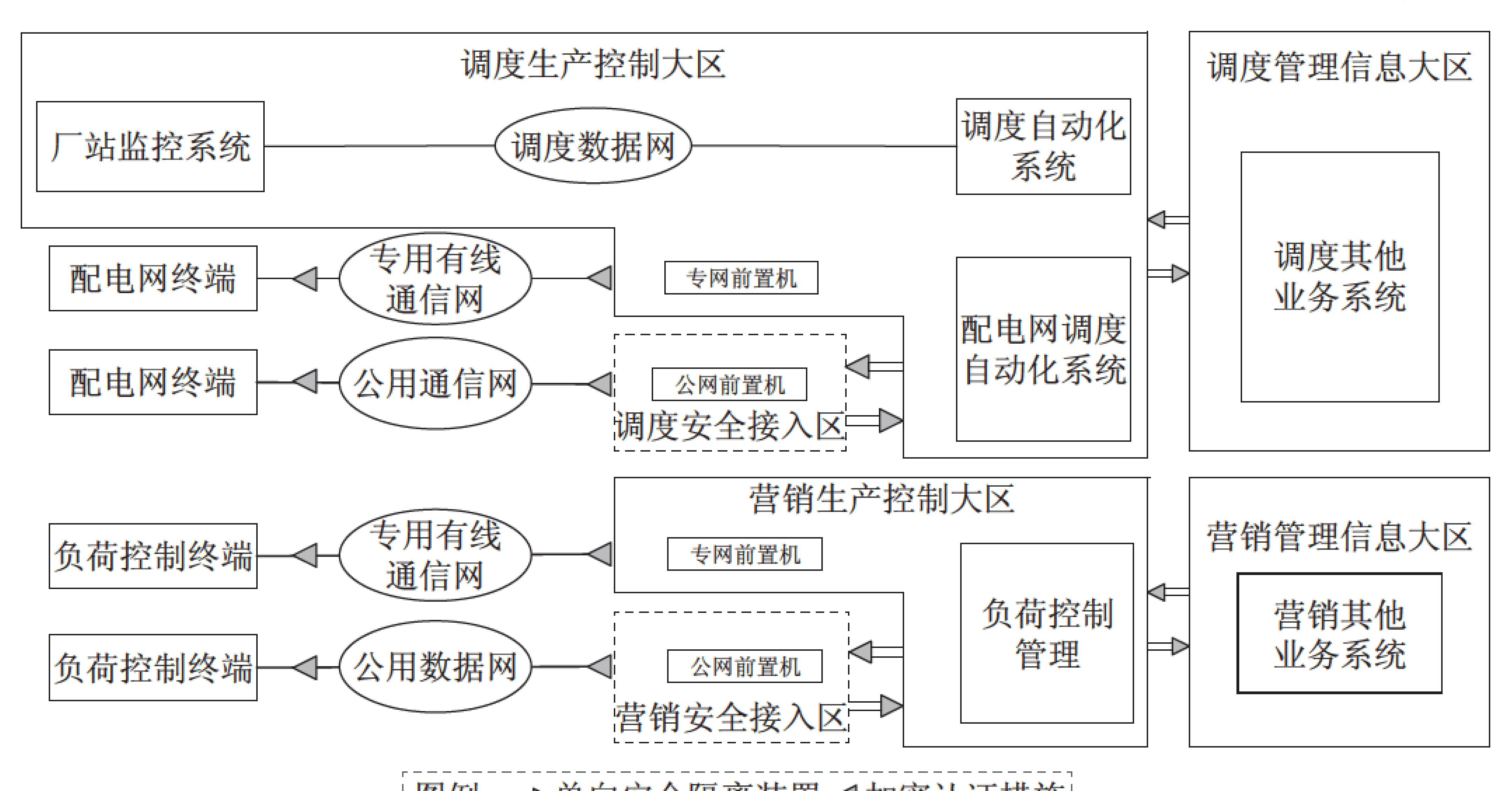


图7-36　安全接入区结构

根据新的安全接入要求，这里采用以下接入方案：

① 对于采用公网、无线专网接入方式的业务，需接入到安全接入区，再经正、反向隔离装置接入到生产控制大区。安全接入区由单向认证模块、通信前置机及正、反向隔离装置组成。

② 接入网关和接入服务器配合，建立加密隧道和通信终端认证机制，进一步保障信息和通信安全。

③ 新的安全方案将无线公网和无线专网划为一类，在进行多业务接入时可采用基于APN/VPN等逻辑隔离方式进行跨安全大区业务隔离，通过安全接入区保障信息安全。

④ 采用有线专网进行多业务接入时，无需经过安全接入区，但对跨安全大区业务仍要进行物理隔离，对同一安全大区业务进行逻辑隔离。

通过数据交互代理技术，实现在安全交换区与内网之间通过专用隔离装置时的报文、数据文件、图像等各种类型实时、批量交换，实现不同安全区之间的数据交换，如图7-37所示。

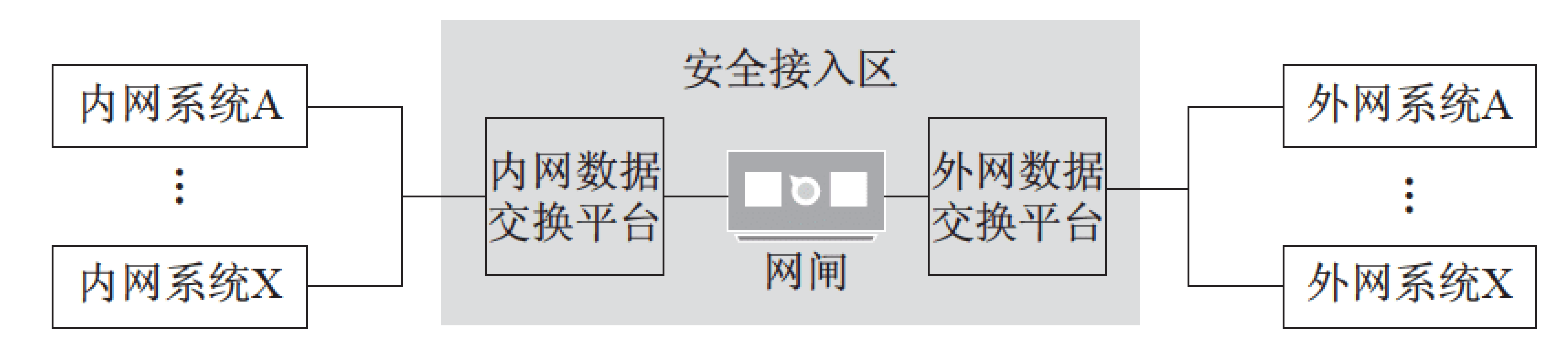


图7-37 不同安全区之间的数据交换

为了不影响原始业务系统的正常运行，安全接入区的数据交换采用前置机策略来进行建设，系统结构如图7-38所示。

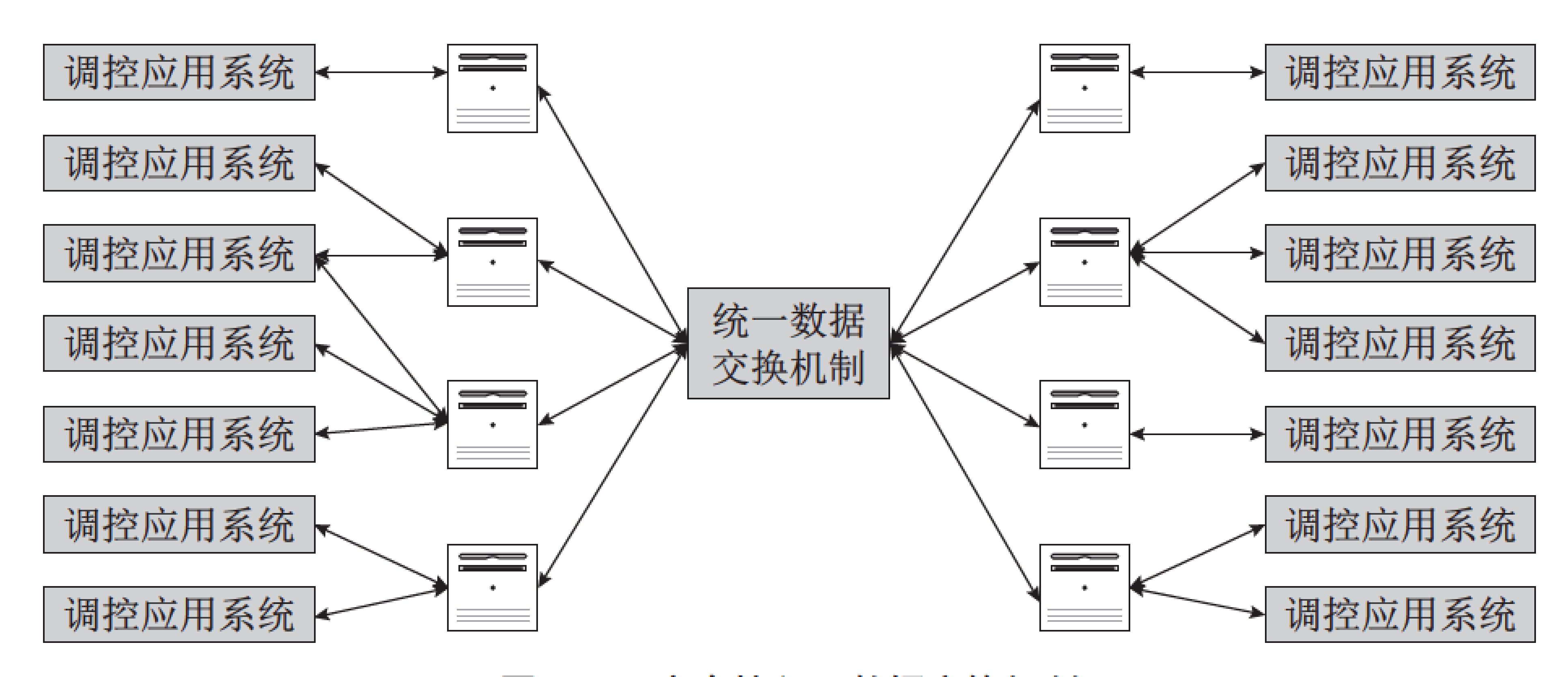


图7-38 安全接入区数据交换机制

在这个体制下，前置机负责与待交换的业务系统以及统一数据交换机制进行沟通，作为数据发送方的前置机，一方面接收发送方业务系统的有关数据，一方面将此数据转交到统一数据交换机制，将信息发送到接收方前置机。接收方的前置机接收统一数据交换机制发送的信息，并将其转交到接收方业务系统。前置机直接与统一数据交换机制交互。在实际项目中，前置机与业务系统可以是一对一、一对多，甚至是多对多等模式，这完全依赖于待进行数据交换的业务系统的数量、待交换数据的规模以及待交换数据的时间频度等情况来进行决定。

安全接入区对外业务的可信接入及基于公钥体系的安全认证技术实现；通过安全接入代理技术，实现正反向隔离交互总线透明信息交换技术。

基于对可信计算的移动终端安全接入模型，按照14号令、36号文要求，建设电力业务数据接入体系的安全标准设定以及相关系统框架；充实和扩展可信网络连接框架，在对可信接入模型研究的基础上，对原有的可信接入方式进行改进，实现了基于可信计算的三步可信认证（用户身份认证、可信平台双向认证以及终端动态完整性度量认证）。

双向身份认证基于可信计算的“信任机制”和“密钥保护”特性，采用基于公开密钥密码学的认证协议，将用户的身份信息、相关密钥信息等由TPM保护，可靠地实现了通信双方的身份认证，并在用户身份认证的基础上，根据可信平台标识唯一性，增加了可信计算平台特有的平台身份认证；实现了从使用者到操作平台的双重认证，可以有效地抵御常用的攻击手段如窃听、重放、假冒、猜测等，具有很强的安全性。

在现有安全接入平台体系下，基于国密算法的移动终端安全加固技术，通过终端加固模型可信引导建立起可信的运行环境。通过以上安全措施，使得不可信的操作系统内核不能启动且不能擅自更改；操作系统的文件系统通过标记进行访问控制，非法主体无法访问敏感客体；网络过滤只允许指定的白名单目标地址可达，即使操作系统存在后门或隐通道，或者木马病毒窃取了敏感信息，也不能将信息送达非法目的地，I/O访问控制封锁了相关USB、网卡等外部设备，保障了敏感信息不能从移动载体泄露，进而达到结果可预测目的。

3. 管理信息大区接入访问控制

管理信息大区是指生产控制大区以外的电力企业管理业务系统的集合，管理信息大区用以支撑公司不涉及国家秘密的企业管理信息业务应用，包括国家电网公司一体化平台、八大业务应用及支持系统正常运营的基础设施及桌面终端。管理信息大区划分为用于承载一体化平台及业务应用和内部办公的信息内外以及用于支撑对外业务和互联网用户终端的信息外网。信息内网与信息外网之间部署逻辑墙隔离设备。管理信息大区的终端接入业务包括用电信息采集、配电管理、营销管理、客户服务管理、电动汽车充电及分布式电源业务等。接入网与信息内网的边界主要指智能电能表、分布式电源终端等采集类终端、移动终端等接入到管理信息大区的边界，信息内外网边界。具体的防护要求包括：

1）访问控制

内网主站业务系统与外网相关业务系统通信时应采用信息内外网逻辑隔离装置。

前置机应配置主站安全模块，或配套配置安全网关、密码机等设备，对终端认证并加密传输数据。

应支持网络与应用层面的访问控制机制。

按照国家信息安全等级保护的要求，根据确定的等级部署边界网络访问控制措施。

对于边界防护设备的策略违背行为应当采取安全审计措施，记录日志并定期分析处理。

不得从任何公共网络直接接入公司内部网络，禁止公网、专网接入通道混用。

2）安全接入

应能够对访问管理信息大区业务终端的身份进行鉴别，只有通过认证的终端才能根据权限访问应用系统。

采集类、移动作业类终端接入管理信息大区时，应建立专用加密传输通道，实现终端身份认证、安全准入和数据安全交换。

3）入侵检测

应按照国家信息安全等级保护的要求，根据确定的等级在纵向网络边界部署边界网络访问控制、信息入侵检测、边界流量监测等安全控制措施。

应采用入侵检测系统对于流经边界的信息流进行入侵检测，入侵检测系统应当对主要的攻击行为进行检测，防止使用常用端口传输恶意信息，防止对服务器发动应用层攻击。

应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击类型、攻击目的、攻击时间，并在发生严重入侵事件时提供报警。

7.10.2 运维支撑工具访问控制设计方案

1. 运维支撑工具的系统结构

为了使运维支撑工具与接入网的访问控制机制相匹配，采用“分区控制，集中展示”的部署模式。

主/被动探针系统采用统一架构设计，如图7-39所示三层平面架构图。

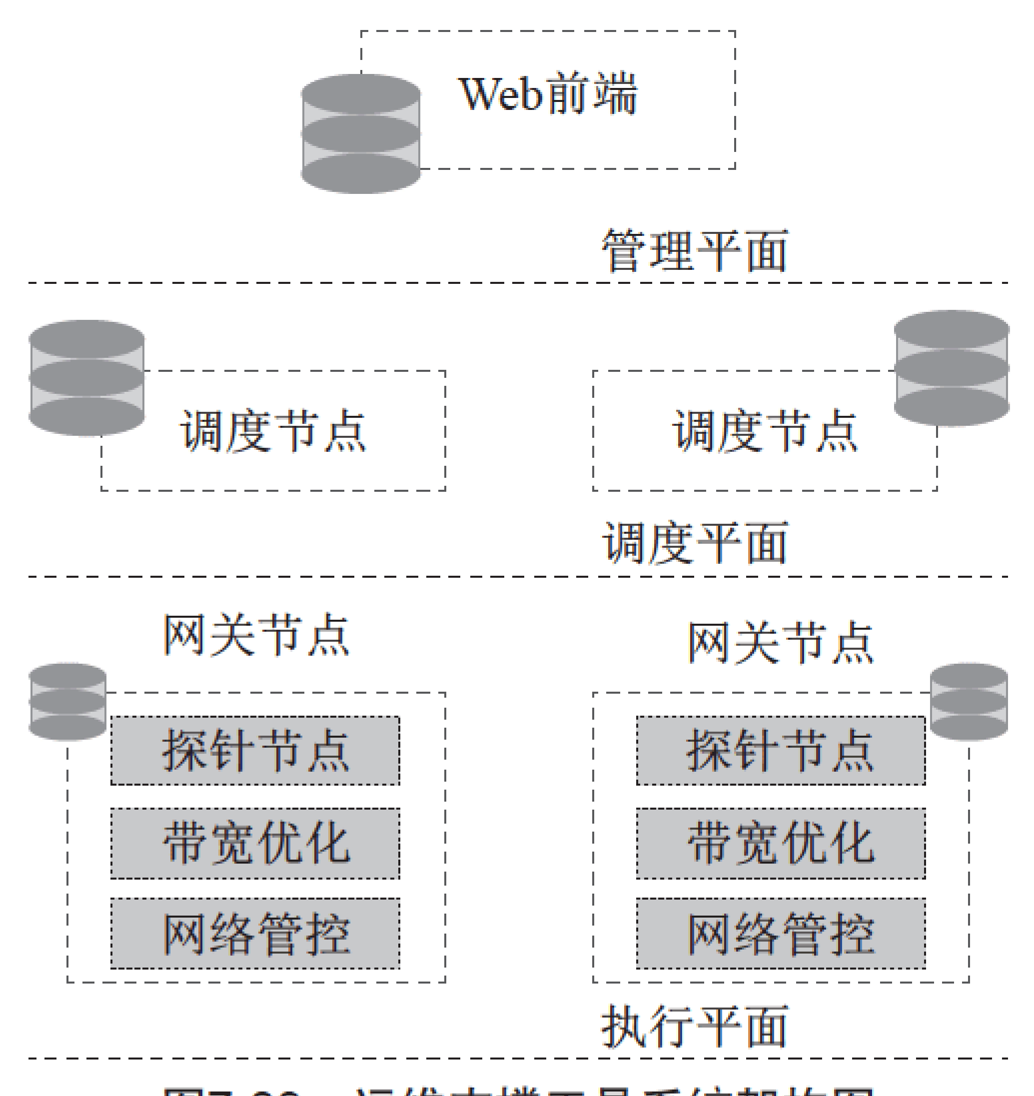


图7-39 运维支撑工具系统架构图

- 管理平面

管理平面主要为系统Web前端平台，提供系统人机交互接口，前端平台通过调度节点控制所有网关节点工作。

- 调度平面

调度平面主要由各个区域的调度节点组成，负责系统上传下达功能，是管理平面与执行平面的桥梁。

- 执行平面

执行平面主要由大量网关节点组成，网关节点是具体任务的执行体。

如图7-40所示，系统由以下四个部分组成：

- 前端管理系统：系统任务调度、结果展示、节点管理的平台，提供人机交互接口；为减少交互请求压力，采用Redis接收处理由调度器和AP发送来的信息数据。
- 调度节点：管理调度域内的探针节点，负责测试任务的调度与结果的收集；可部

署多级调度节点。

- 数据存储检索：支持海量的不同类型数据结果存储，提供快速、灵活的检索接口，支持外部系统检索。
- 探针节点：从用户侧感知网络性能，执行网络具体测试任务，获取测试结果，支持测试工具的快速部署与输入/输出模板标准化。

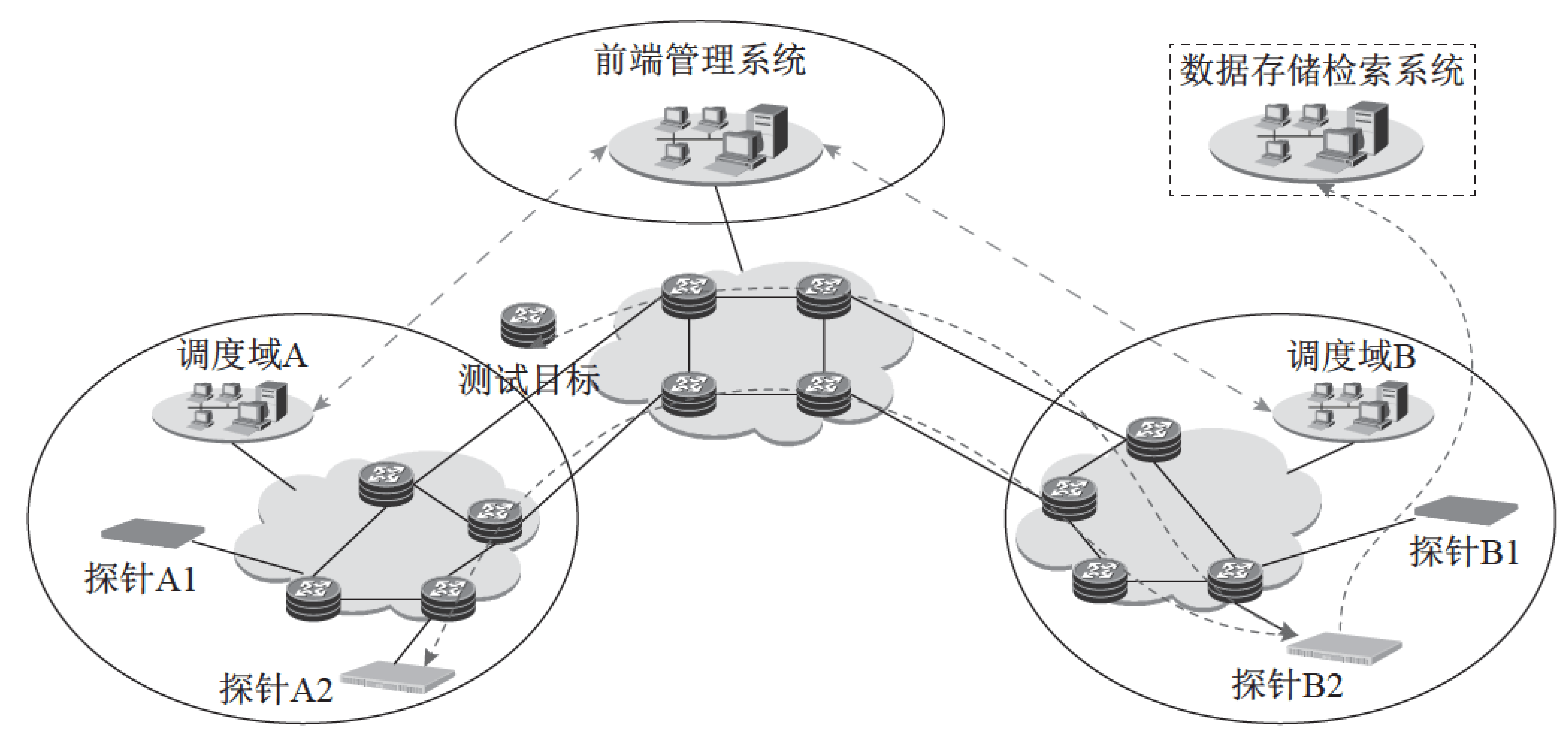


图7-40　运维支撑工具系统部署结构图

图7-41所示为分布式节点调度框架，系统采用分布式结构，通过负载均衡进行资源的合理分配，实现海量节点的调度运行。

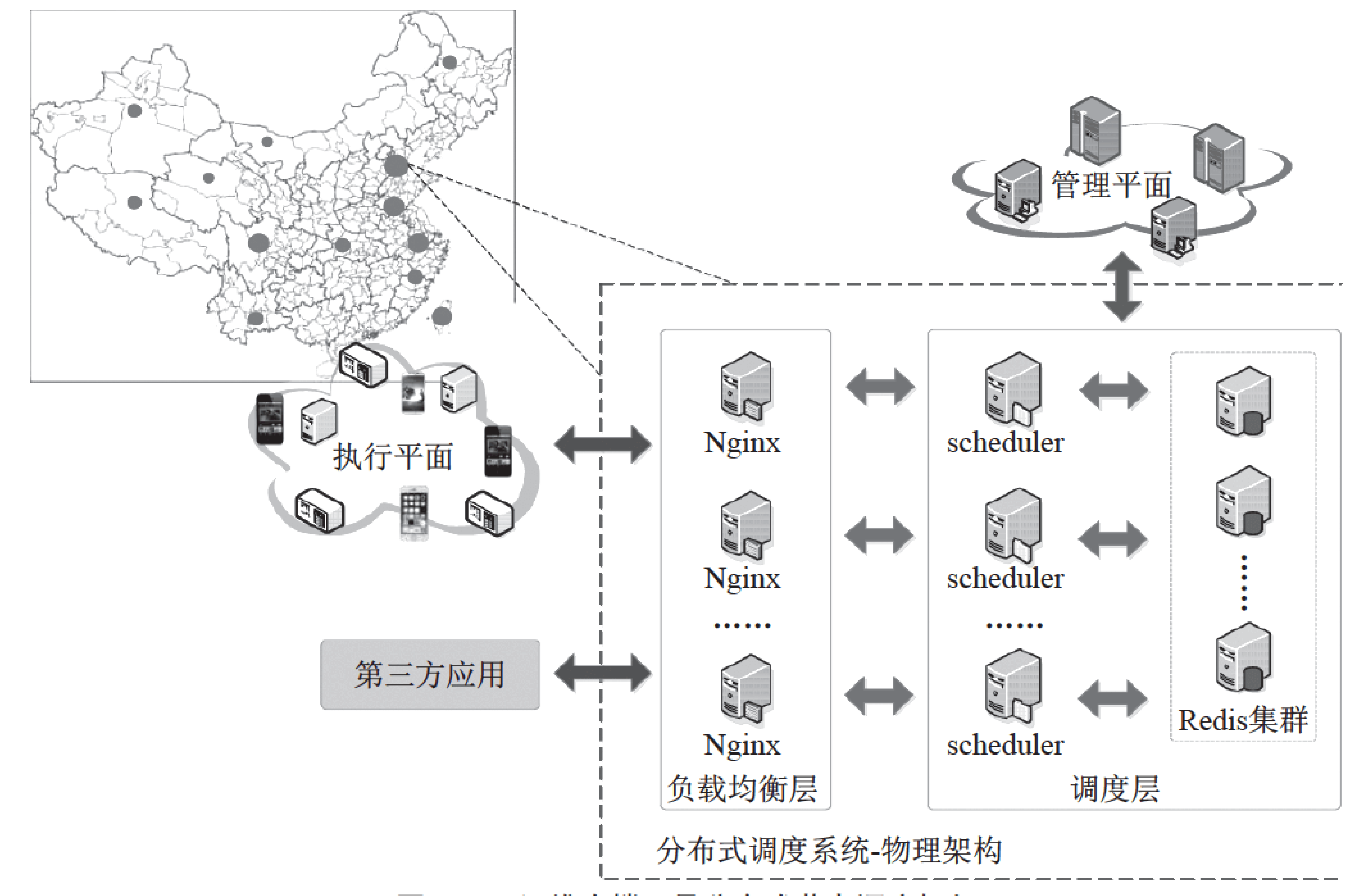


图7-41　运维支撑工具分布式节点调度框架

2. 运维支撑工具部署方案

运维支撑工具分为前端管理系统、调度节点、数据存储检索和探针节点四个模块。

考虑到终端通信接入网中生产控制大区和管理信息大区的隔离，在生产控制大区和管理信息大区分别部署一台服务器，安装前端管理系统、调度节点和数据存储检索模块。生产控制大区服务器上部署三个调度节点分别调度以太网、EPON网络和无线专网的探针节点，在无线公网部署一台前置机，安装调度模块调度无线公网的探针节点，前置机通过安全接入区连接生产控制大区服务器。管理信息大区服务器部署一个或多个调度节点调度数据网中的探针节点。生产控制大区服务器通过单向物理隔离装置向管理信息大区服务器报送运行信息，管理信息大区服务器集中显示全网数据，起到运维支撑工具主服务器的作用，如图7-42所示。

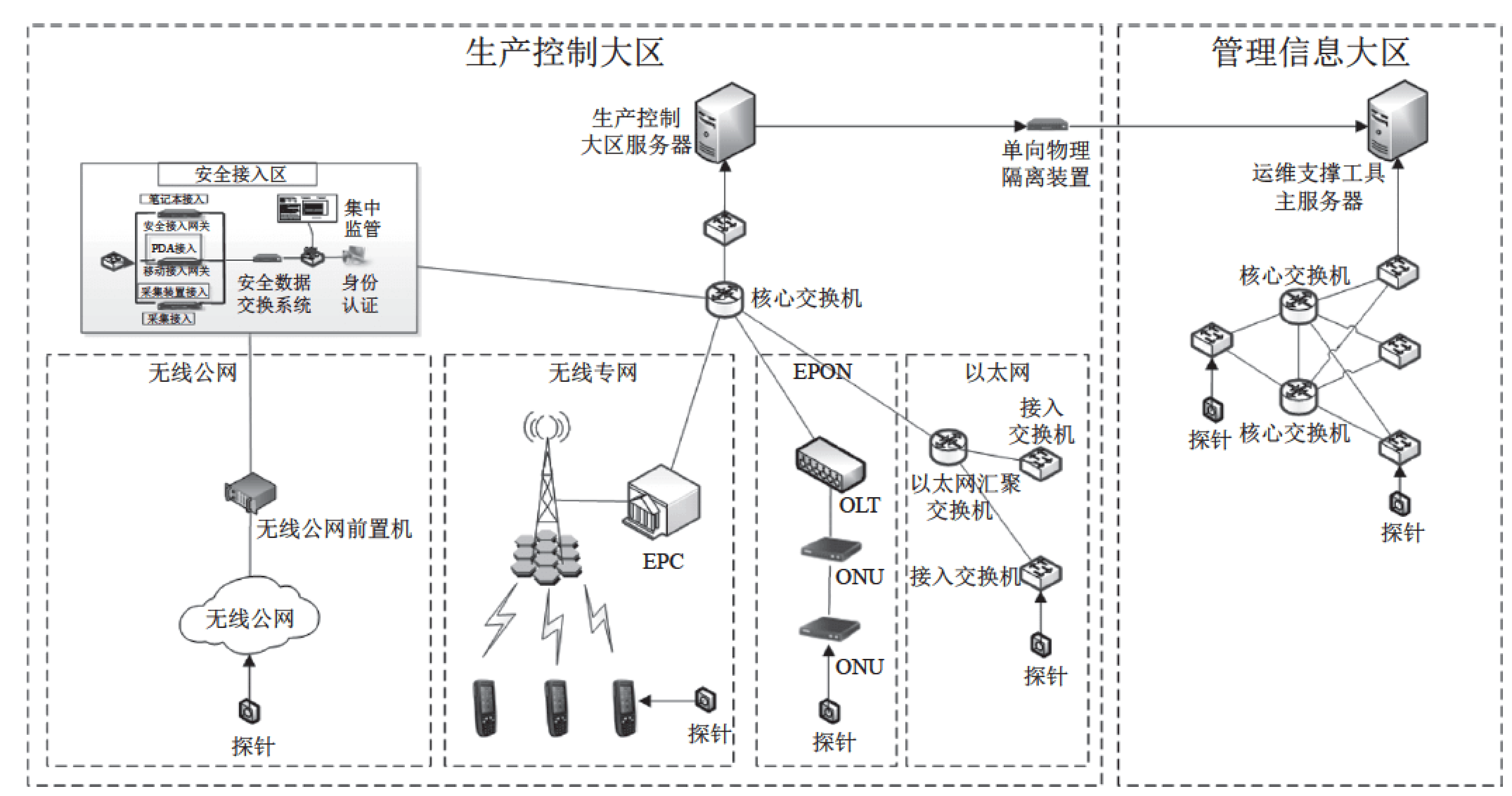


图7-42 运维支撑工具部署图

1） 以太网访问部署方案

如图7-43所示，以太网调度节点部署于生产控制大区服务器，探针节点部署于数据网的末端节点，尽可能多地覆盖数据网链路。

2） EPON网部署方案

如图7-44所示，EPON网调度节点部署于生产控制大区服务器，探针节点部署于EPON的末端ONU及OLT上，对EPON网络内部情况能较好地进行探测。

3）无线专网部署方案

如图7-45所示，无线专网调度节点部署于生产控制大区服务器，探针节点部署于无线终端CPE和核心网EPC上，对CPE到EPC的无线环境，以及EPC接入数据网的链路情况都能进行探测和故障定位。

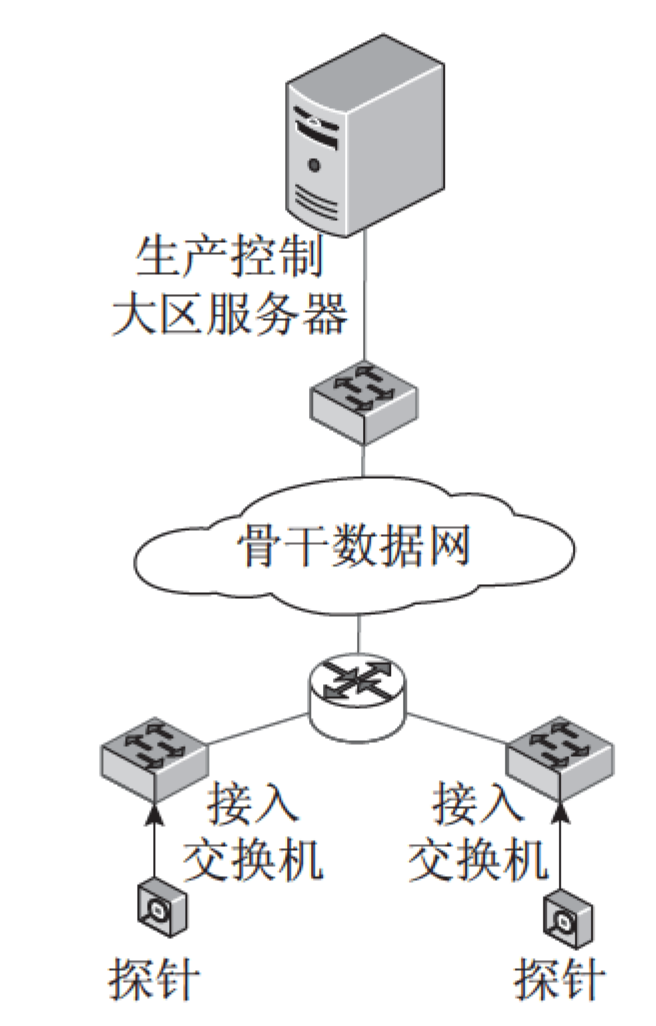


图7-43　运维支撑工具以太网部署图

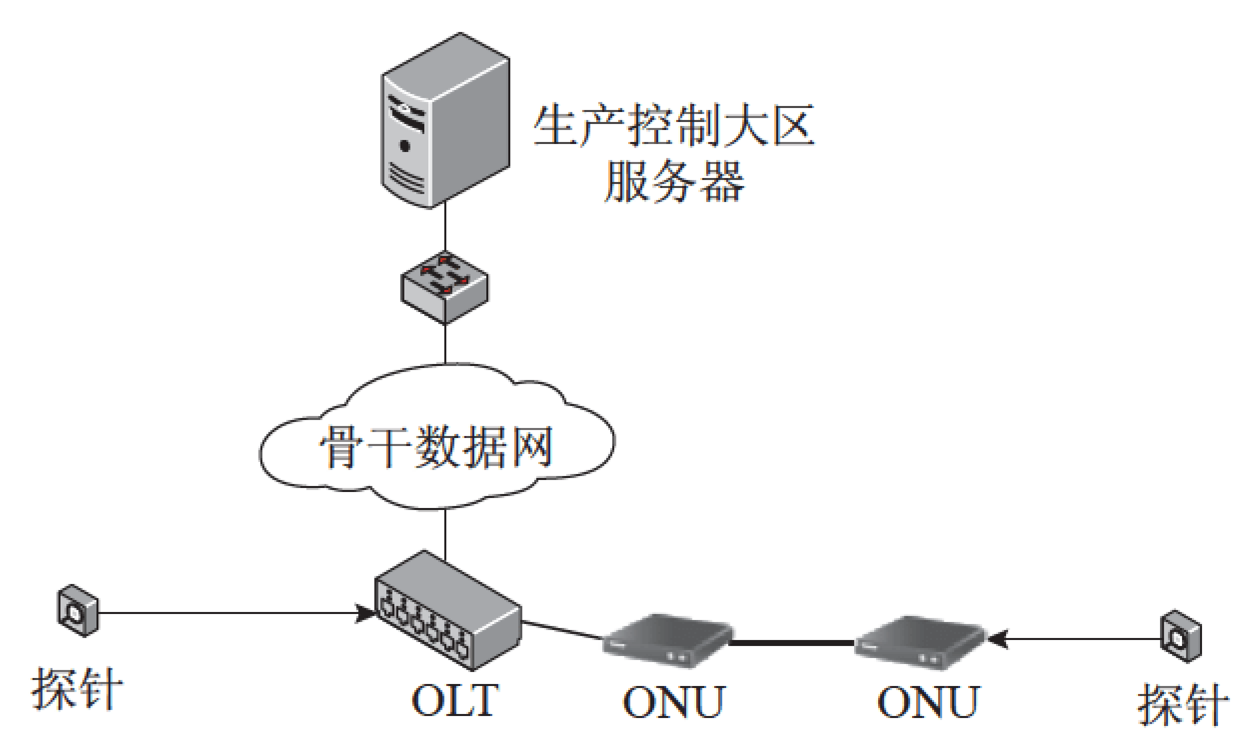


图7-44　运维支撑工具EPON网部署图

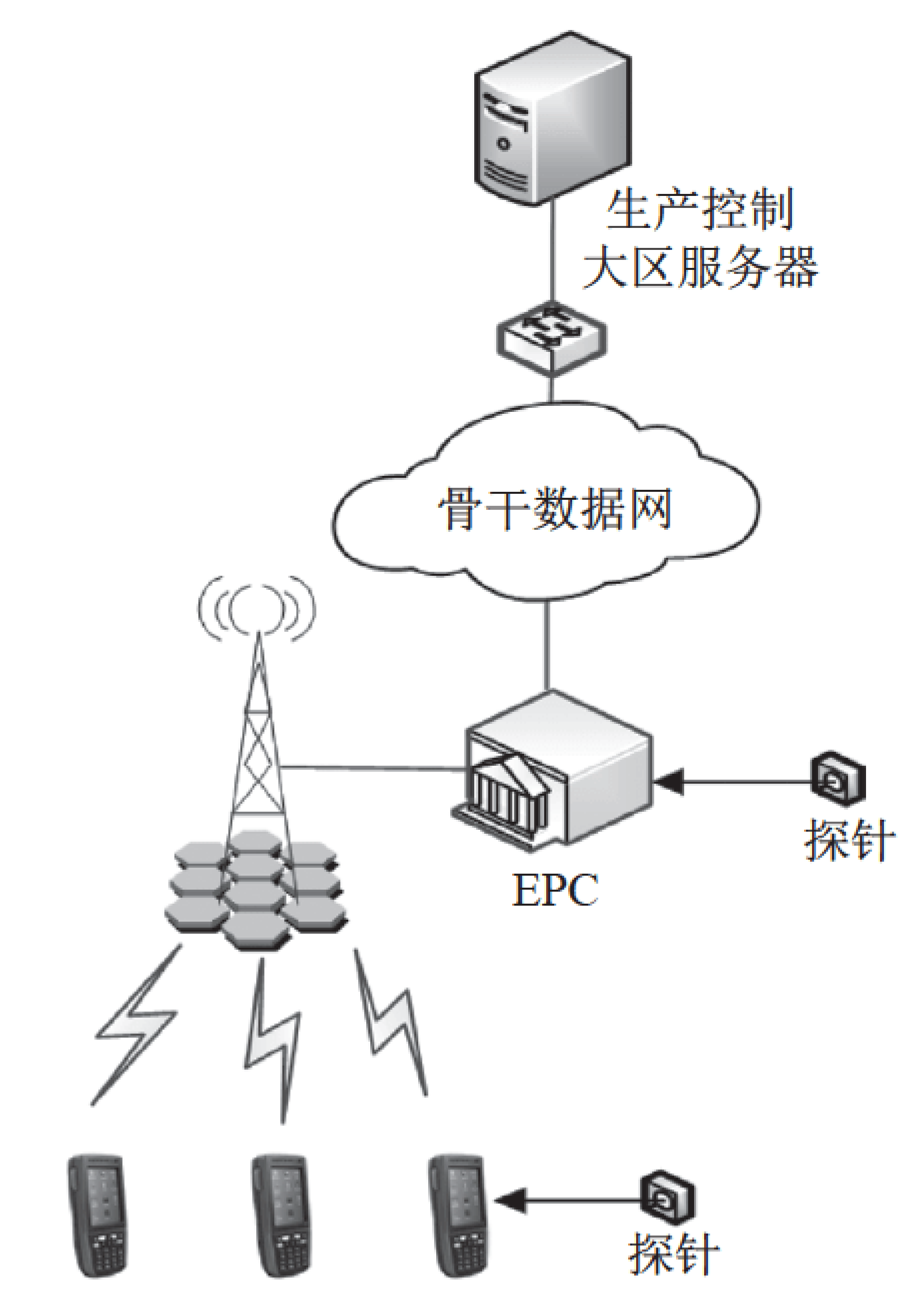


图7-45　运维支撑工具无线专网部署图

4）无线公网部署方案

如图7-46所示，无线共网调度节点部署于安全接入区前的前置机上，探针节点部署于无线终端CPE，重点对CPE到电力通信网所经过的运营商无线环境和有线环境进行探测，由于探测数据包无法通过安全接入区，因此在安全接入区前安装前置机部署调度节点，调度节点通过安全接入区连接部署于生产控制大区服务器上的运维支撑工具前端管理系统。

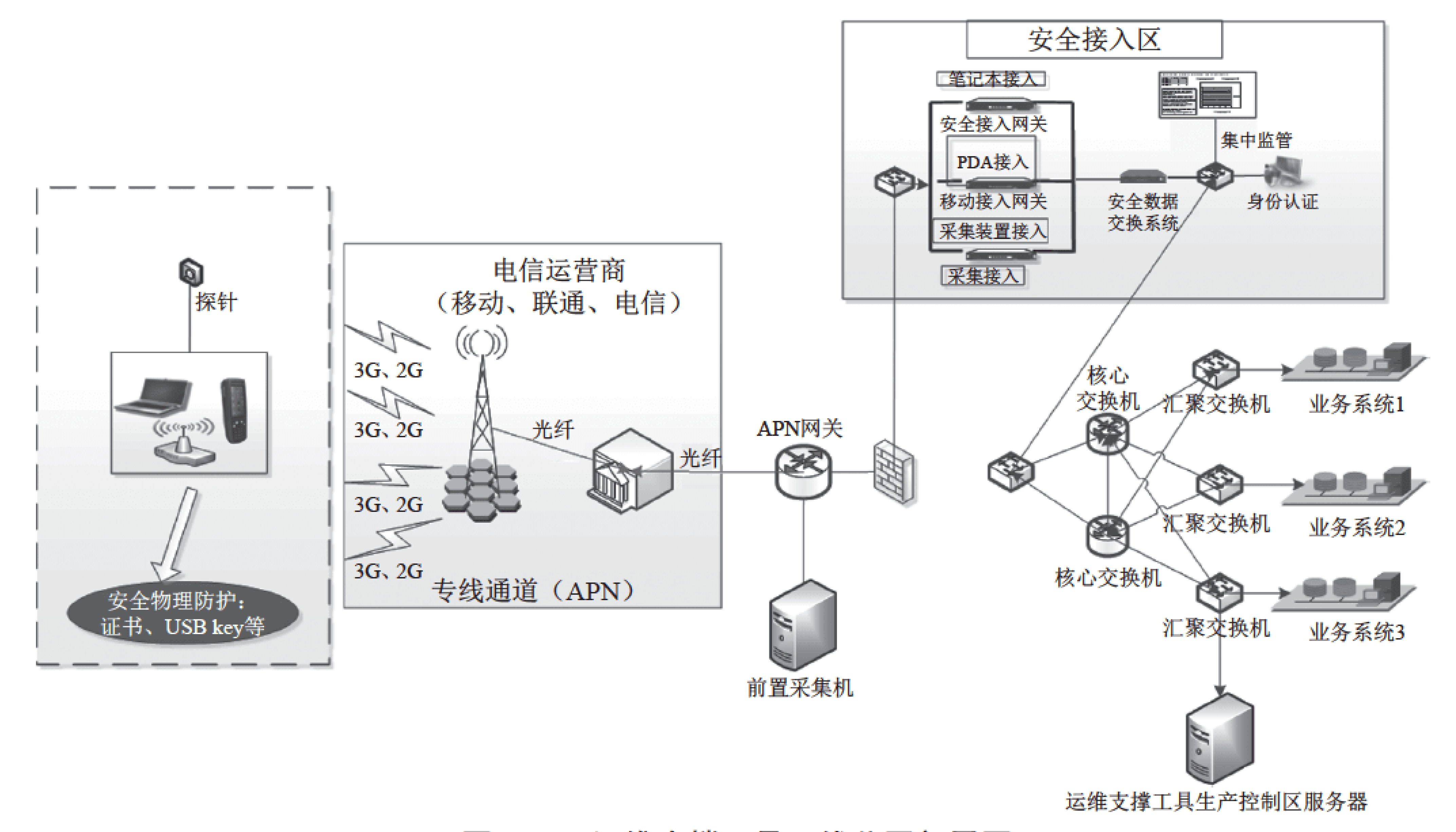


图7-46　运维支撑工具无线公网部署图

7.11 总　结

本章主要针对电力终端通信接入网的运维进行分析，主要讨论了四个部分：

第一部分（7.1节和7.2节）主要介绍了行业内和行业外的接入网技术要求，然后又介绍了几种重要的网络流量分析方案。这几种方案各有优缺点，并且各个方案之间并不是互斥的，一个方案可能是在另一个方案基础上的优化改进，也可能是一种技术的两种方式。

第二部分（7.3节～7.5节）主要解决终端通信接入网的问题，利用分布式探针的主动测量技术提高终端通信接入网的故障节点快速定位能力。项目首先在网络性能评价指标选取原则的基础上构建了网络性能指标体系，进而详细介绍了网络性能指标，提出了网络性能探测技术，用于探测网络的性能。在网络性能分析的技术上，项目研究了基于探针的综合故障定位技术方案，包括故障检测的探测选择技术和故障定位的探测选择技术。最后研究了网络性能保障机制，保证终端通信接入网基础设施、业务和流程能够正常、经济、可靠、安全地运行，从而增强企业的服务能力，提升服务水平。

第三部分（7.6节～7.8节）针对终端通信接入网的关键问题提出了典型的应用场景以及探针部署模式，研究了面向资源优化的分布式智能测量探针监控部署策略、面向动态业务的监控策略调整以实现电力场景与探针技术的适配关联，并深入探讨了基于主动探测技术的故障定位。

第四部分（7.9节和7.10节）针对运维支撑工具的研发，研究了对网络进行评价所需的监控指标及其展现模式，运维支撑工具物理、网络、设备、应用、数据等各层所需采取的安全防护和权限管理策略，以及为了在终端通信接入网部署运维支撑工具设计的前端—调度节点—探针节点三级分布式的系统架构和部署结构，并针对以太网、EPON、无线专网、无线公网四种接入方式分别做了具体设计。

第8章

电力终端通信接入网新技术展望



8.1 新型通信技术的研究

8.1.1 可见光通信技术

1. 概述

可见光通信技术（Visible Light Communication，VLC）是无线通信技术和光纤通信技术结合的产物，是一种利用可见光作为信息载体的通信技术。从通信的有效距离来看，可见光通信可以分为室外远距离可见光通信和室内近距离可见光通信两种。现阶段室外远距离通信大都基于红外线激光二极管。室内近距离可见光通信技术一般使用用于照明的发光二极管（Light Emitting Diode，LED）作为信息光源，实现几米之内的信息传输，通过调制技术控制LED亮度实现室内照明的同时完成数据通信。

可见光通信技术通常运用强度调制和直接解调（Intensity Modulation/Direct Detection，IM/DD）技术，在接收端利用光电传感器进行数据传输的无线通信技术。以LED灯作为互联网接入热点，半导体光照明通信系统在实现方式上通常由网络接入控制器、民用级照明LED灯和接收机三部分组成。通常安置在LED灯前端的接入控制器通过以太网、卫星网络等方式连接外部网络，并将LED驱动电信号转换成为光信号，使得LED以照明功率变换调节的方式实现数据下行传输，接收机将光信号转换为电信号发送给用户，用户端通常还需要集成红外或者射频模块，以实现上行数据传输。VLC是一种更加绿色的通信方式，主要技术优点包括：

（1）光源内在的调制性：利用光源功率控制和明暗调节作为调制方式。因光源部署方便，可见光通信是室内最后 1 m通信方案的理想解决方案。

（2）保密性：在可将光通信中，“所见即所得”，光线传播方往往具有指向性，传输过程中窃听者无法透过墙壁等遮蔽物体进行信息获取。

（3）无频谱许可要求：传统无线电频谱资源十分有限，而可见光光谱一般为380～780nm，工作频段无须授权。

（4）电磁兼容性好：与射频信号互不干扰，可以应用在复杂的电磁环境中（如机舱

和医院等）。

（5）安全性：较射频通信来说，可见光通信不会产生电磁辐射，合理照明功率下对人体健康没有损害。

相比于传统的无线通信技术，VLC技术结合照明和通信，利用光作为载波很好地解决了射频通信中无线频谱资源紧缺这一难题。可见光通信可在照明的同时进行通信，扣除照明本身的能耗，用于无线信息传输的能耗显著低于传统射频无线通信系统。

2. 基本原理

可见光通信链路拓扑结构的研究中相对比较成熟和稳妥的做法是按照红外通信信道链路方案进行设计，根据发送和接收机之间的相对位置分为视距（Line of Sight，LOS）传输链路、散射传输链路（Diffuse Links）和准散射传输链路（Quasi-Diffuse Links）。视距传输链路是指发送端和接收端之间直接存在无遮挡的光传播路径，IrDA标准中的快速红外（Fast IR）4 Mbps链路便是典型的视距点对点传输链路。与其他链路结构相比，视距链路VLC系统拥有链路效率、信道传输带宽（普通LED光源LOS信道传输3dB带宽约为16～20MHz）等优势。这是因为该系统发射机和接收机通常需要严格的光学对准，也使得光电检测管的视场角可以设置得足够小，极大地减少了噪声光源的影响。在此基础上利用空间分集复用技术，利用并行视距传输链路使得传输速率达到50Mbps。另一种并行视距传输链路VLC系统运用自由空间通信跟踪、瞄准技术，为室内移动终端提供155Mbps的传输速率。在实际场景中，由于视距链路容易受到障碍物和阴影的阻断，因此这类VLC系统通常应用在短距离室内光通信应用之中，并且信道具有时不变或者慢时变性，性噪比通常比较高。

散射和准散射传输链路是指光线利用物体和墙壁等表面反射到达接收机的路径。这种链路结构不仅仅要考虑到收发机光电元器件特性的限制，还需要加入因多径散射而引起的类似于低通滤波的失真。在众多可见光信道模型中，这一因多径色散引起的信号畸变被建模成慢时变线性过程。与传统射频无线信道不同的是这里的多径传播并不会产生衰落（fading），原因是接收端光电二极管的元器件尺寸要远大于可见光波长，为发送信号提供了空间分集增益。接收信号大小仅与光电转换器表面积上接收的光功率成正比，在接收机静止或者波长长度级别的移动下，接收信号大小并不会有实质性的改变。散射和准散射传输方式下收发端无须跟踪对准，降低链路设置难度，也更符合实际应用场景。通过弥散光信道传播方式运用计算机仿真室内时变多径光信道进行响应，对所有只包含一次反射路径到达接收机的信道进行建模。这一模型将室内物体表面分割成一系列光线反射单元，并假设光源和这些反射单元的辐射模式为朗伯（Lambertian）辐射模型，光源表面上任意角度的光强可以写成：

$$I(\theta,\phi,n)=\frac{n+1}{2\pi}P_c\cos^n\phi[W/sr] \tag{8-1}$$

其中P_c是光源中的照度，$n=\ln 2/\ln(\cos\theta)$为辐射阶数，$\phi\in[-\pi/2,\pi/2]$和$\theta\in[0,\pi/2)$分别代表点到法线平面的极化角度和方位角度。室内空间任意点(x,y)的水平照度为：

$$I_{(x,y)}=I(\theta,\phi,n)/d^2\cos\psi \tag{8-2}$$

直流增益为：

$$H_{DC}=\frac{n+1}{2\pi d^2}P_c\cos^n\phi T_s(\psi)g(\psi)\cos\psi, 0\leqslant\psi\leqslant\psi_{con} \tag{8-3}$$

其中$\cos^n\phi$为接收机入射角度，ψ_{con}为接收机可视角度，d为光源和接收机表面距离，$T_s(\psi)$为发送端滤波增益，$g(\psi)$为接收机增益。这里H_{DC}是LOS直流响应增益，模型中需要继续计算第一次反射路径的信道响应并叠加。实际上，一条光线反射达到三次之后接收端PD就几乎收集不到它的能量。

3. 关键技术

（1）可见光通信系统的信道容量研究

光通信研究中光能量信道通常假设为泊松计数（Poisson Counting）信道。假设信道噪声为高斯分布，推导无光功率约束情形下的信道容量，利用多进制调制方案验证了光信道高速可靠传输的实现。在信道容量推导中加入瞬时光功率约束条件，并验证此时二进制调制方案的最高传输速率接近信道容量。实际上，泊松计数信道噪声也应当假设为接收机单位时间内接收到的噪声光源光子数，因此光信道容量的推导和求解要难于传统射频信道模型。即便将信道噪声的概率分布简化为高斯（Gaussian）分布，在瞬时和平均光功率约束条件下，能够达到信道容量的发送信号最佳概率分布也总是离散表达形式。针对不同调制，计算视距传输下无码间干扰时泊松计数信道M阶脉冲位置调制（Pulse Position Modulation，PPM）最大传输速率。在此基础上，加入了光散射信道并给出存在码间干扰下时的M阶PPM调制的最大可实现传输速率。首先假设每个符号的光功率为定值，在平均光功率约束条件下推导出多载波调制下的信道容量的上界。接着作者假设系统模型满足光功率约束和信号带宽约束条件，通过空间球体填充理论推导得出更为精确的泊松计数信道的信道容量上下界。假设系统中信噪比较高，噪声为高斯分布且与信号不相关。

（2）可见光通信系统的接收机研究

在VLC系统中，干扰与噪声的波长约为接收机尺寸的10^{-3}级别，因此在光通信中并没有明显的多普勒频移，经典的接收跟踪算法并不适用于该系统。VLC系统通常使用PD作为接收机，大体可以分为两类：一类是PIN型PD，这一类PD具有耐温性高、成本低、强光下性能优异等特性，使得它成为主流PD类型；另一类为雪崩（Avalanche）PD，在入射光强较弱时该PD性能优于PIN型。VLC系统中典型的PD响应度曲线峰值为800nm且对红色光谱更加敏感。RGB三色分别运用于VLC系统时，传输速率与性能并不相同，红光波段有着更高的频率响应特性和传输速率。总的来说，接收机的配置与布局有三类：一类是广泛使用在VLC系统中的单一接收机；第二类是选择性合并接收机，但实验表明该类接收机

性能仅略好于蓝光滤光方案，接收机复杂度却高出很多，所以并没有得到广泛使用；第三类是成像分集接收机，利用PD阵列和透镜组合对每个光源进行区分和对准，这类接收机特别适用于光MIMO方案。VLC系统使用成像接收方法利用 4 发 9 收接发机实现了单路250Mbps、总速率1.1Gbps的传输速率；通过使用角度分集接收机来解决没有LOS传输的漫射信道VLC系统传输问题。

（3）可见光通信系统的调制技术

针对IM/DD信道的特点，大量经过改进的射频调制方案被运用到可见光通信系统中，主要包括脉冲类调制方案和多载波调制方案。脉冲类单载波方案实现简单，适用于无需复杂的信道均衡的LOS传输情形，主要包括开关键控（On-Off Keying，OOK）、色移检控（Color Shift Keying，CSK）、脉冲幅度调制（Pulse Amplitude Modulation，PAM）、脉冲位置调制（PPM）和脉冲宽度调制（Pulse Width Modulation，PWM）等广泛应用于射频通信中的调制技术。

多载波调制方案主要用于散射传输链路情况，利用多载波频域均衡简单的优点来对抗多径。目前多载波的方案主要有：直流偏置光OFDM（DC-biased Optical OFDM，DCO-OFDM）和非对称截断光OFDM（Asymmetrically Clipped Optical OFDM，ACO-OFDM），除此之外，还有其他一些变化形式，如脉冲幅度调制一离散多音（Pulse Amplitude Modulation Discrete Multi-Tone，PAM-DMT）、位置调制OFDM（Position Modulating OFDM，PM-OFDM）、单极性OFDM（unipolar OFDM）和反转OFDM（flip-OFDM）等。

目前可见光通信的多载波调制方式的研究主要集中在DCO-OFDM、ACO-OFDM和PAM-DMT上，总体来说在相同载波数和调制阶数下，若信噪比条件相同，则ACO-OFDM调制方式误码率性能最优，带宽效率最差；相同传输速率下，PAM-DMT和DCO-OFDM所需的调制阶数最少，但PAM-DMT的误码率性能要优于DCO-OFDM，随着调制阶数的增加，DCO-OFDM方案带宽效率优势逐渐明显。比较得出对于传输带宽受限系统，应该优先考虑DCO-OFDM调制方案；对于光功率受限系统，应当优先考虑ACO-OFDM或者PAM-DMT调制方案。

（4）可见光通信系统中的多输入多输出与多址技术

多输入多输出（Multiple input Multiple output，MIMO）技术被视为下一代无线通信系统的关键技术之一，这一多天线技术在光传输系统中也得到一定的研究和扩展。光多通道传输技术已经在无线光通信、芯片级（chip-to-chip）互联和全息存储系统中得到广泛应用，利用空间分集复用成倍地提高了数据吞吐量。多通道技术最先被引入到远距离自由空间光通信中，并得到广泛的研究和应用。自由空间光信道容易受到阴影、大气湍流等因素的影响而产生衰落。目前对抗光信道衰落的方法主要有差错控制编码技术、MIMO空时分集技术等。

自由空间光通信系统大都采用相干调制，在幅度和相位空间两维自由度上设计的

MIMO空时传输方案并不能直接应用到室内IM/DD可见光通信之中。目前商用LED的白光调制带宽仅有几兆赫兹，即使采用滤波后的蓝光通信，可用带宽也最多在20MHz左右，而且滤波损失了一部分接收信号的能量。要在有限带宽内取得高的传输速率，就需要用到包括多载波调制OFDM以及MIMO技术在内的多种先进通信和信号处理技术。可见光MIMO技术中发送端使用阵列光源，接收端设置多个光电检测管，信号合并所得到的接收分集增益提高了信噪比，优化了系统性能。除此之外，光MIMO技术中多个近似互相独立的并行子信道还可以为系统提供空间分集增益，能有效地对抗光信道频域选择性，大大降低信道同时衰落的概率，提高传输可靠性。光通信中光源角度分集需要接收机精确地对准和跟踪，利用对准和角度分集技术实现了4m距离内70Mbps的传输速率。另一种可见光MIMO技术是接收光电二极管利用光学成像透镜使得每个光源得以辨别和区分，减少非对应光源的噪声干扰。显示光学成像接收机可以获得13dB以上的光功率增益。

光MIMO信道与射频MIMO信道相关技术不同，VCL系统的接收机阵列尺寸远大于波长确保信道矩阵满秩。非成像VLC-MIMO系统可以利用足够大的接收阵列使得光源在接收机上的镜像没有明显重合。在成像MIMO系统中，这一类信道干扰可以通过调整接发两端位置和增加接收机数目进行抑制。在VLC系统实际实现中秩亏的信道矩阵仍然需要考虑，因此光源位置和数量需要设置和调整使得信道矩阵满秩。成像系统的LED阵列尺寸仿真中指出，随着发送端光源数目和尺寸的增加，所需的光电检测管与透镜尺寸都需要增大。一个6×6的MIMO系统需要的检测阵列尺寸为5.91cm×5.91cm。尺寸对于固定基站来说是可行的，但是对于移动终端来说并不合适。虽然大尺寸的接收阵列可以在提高传输速率的同时提供更加准确的信道矩阵，但是同时也增加了接收端复杂度。实际室内VLC应用场景中往往因为遮挡和散射使得信道矩阵条件很差，系统误码率性能严重下降，多输入单输出（Multiple-Input Single-Output，MISO）技术可以作为一种可行的解决方案。

由于可见光传输系统的特殊性，VLC系统MIMO空时编码设计仅能利用信号幅度这一维空间，极大限制了MIMO性能的发掘。MIMO技术与空间分集（spatial diversity）首先运用在自由空间通信（Free Space Optical，FSO）；接着研究室内环境下利用漫射信道进行传输的VLC系统，给出了像素MIMO无线光通信系统并分析了该光MIMO的信道容量；提出了利用空间维度来设计IM/DD光通信空时编码，将空间调制（Spatial Modulation，SM）用于VLC系统MIMO传输方案。利用空间维度，空间调制每次选择LED阵列中的一个或者一组来发送数据。由于空间调制减少了瞬时光通路的数目，这样也就避免了信道间的互相干扰，同时接收端检测到某个或者某LED发送组合选择这一操作本身也携带了编码，因而提高了系统信息传输速率。最初的空间调制光通信并没有编码，打孔卷积码在光通信中的应用带来不错的性能提升。在此基础上又提出了将网格编码调制（Trellis coded Modulation，TCM）与空间调制结合的TCSM方案，进一步提高了MIMO系统性能。TCSM将信息比特分成两部分，一部分用于选择LED，另一部分则用于选择传输的星座点。

8.1.2　NB-IOT

1. 概述

现有物联网通信技术包括非蜂窝技术和蜂窝技术两大类。其中，非蜂窝技术主要以短距离WiFi、蓝牙为主，也包含Sigfox和LoRa蜂窝技术，主要以 2G/3G/4G网络应用为主。目前，运营商的市场主要集中在蜂窝技术领域。

NB-IoT是由3GPP定义的基于蜂窝网的窄带物联网技术，支持海量连接，有深度覆盖能力、功耗低、适合传感计量、监控等物联网应用，还可适用于智能抄表、智能停车、车辆跟踪、物流监控、智慧农林牧渔业以及智能穿戴、智慧家庭、智慧社区等，这些领域对广覆盖、低功耗、低成本的要求非常明确，目前广泛商用的2G/3G/4G技术及其他无线技术都无法满足这些挑战。

2. 基本原理

（1）工作模式

NB-IoT目前只支持FDD传输方式，带宽180kHz，支持3种工作模式，如图8-1所示。

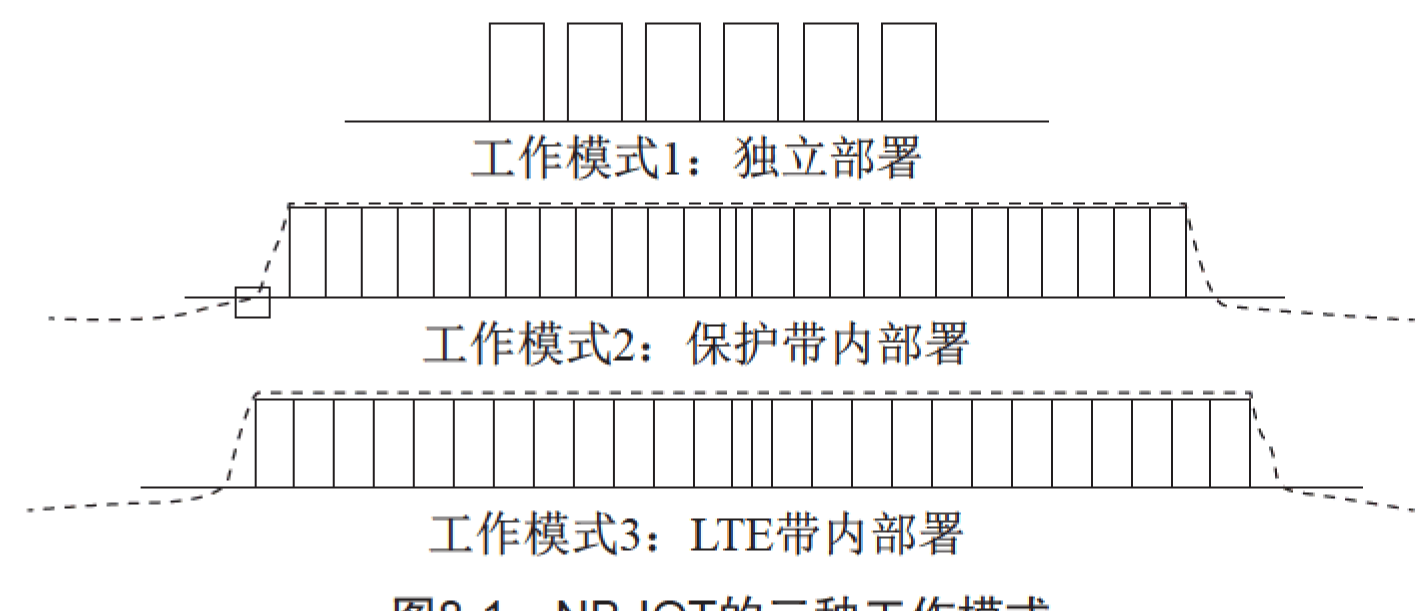


图8-1　NB-IOT的三种工作模式

- 独立（stand alone）部署，不依赖LTE。
- 保护带内（guard band）部署，不占用LTE资源。
- 带内（in band LTE）部署，占用LTE 1个PRB。

其中，虽然保护带内部署没有占用LTE频率资源，但因为设备复杂度最高，射频指标最严格，而系统性能却和LTE带内部署模式类似，因此产业发展较慢，目前仅个别设备与终端芯片厂商支持，存在部分设备与终端芯片并无支持计划的情况。

（2）传输方式

NB-IoT支持下行OFDMA传输，频域每个载波只包含一个 PRB子载波间隔，15kHz CP（Cyclic Prefix，循环前缀）长度为常规CP。

上行定义了单子载波（Single-Tone）和多子载波（Multi-Tone）两种传输方式。其中，单子载波支持两种子载波间隔，3.75kHz和15kHz。对于15kHz 子载波间隔定义了12个连续的子载波；对于3.75kHz子载波间隔，定义了 48个连续的子载波；多子载波传输支持

15kHz的子载波间隔，定义了12个连续的子载波，这些子载波可以组合成3个、6个或12个连续的子载波。

因为功率谱密度高，所以相同TBS下，3.75kHz覆盖能力大于15kHz。15kHz 小区容量是3.75kHz的92%，但调度效率和调度复杂度优于3.75kHz。由于 NPRACH必须采用3.75kHz单子载波传输方式，因此，目前大多数设备上行优先支持3.75kHz单子载波传输方式。在引入15kHz单子载波传输和多子载波传输方式之后，会根据终端信道质量自适应地进行选择。

下行业务信道NPDSCH传输的最小调度单位是RB（Resource Block）。上行业务信道NPUSCH 传输的最小调度单位是RU（Resource Unit）。时域上，对于单子载波传输3.75kHz，子载波间隔时资源单位为32ms，15kHz子载波间隔时资源单元为8ms。对于多子载波传输3个子载波，间隔时为4ms，6个子载波间隔时为2ms，12个子载波间隔时为1ms。

（3）帧结构

NB-IoT eNode B下行支持E-Utran无线帧结构1（FS1），如图8-2所示。

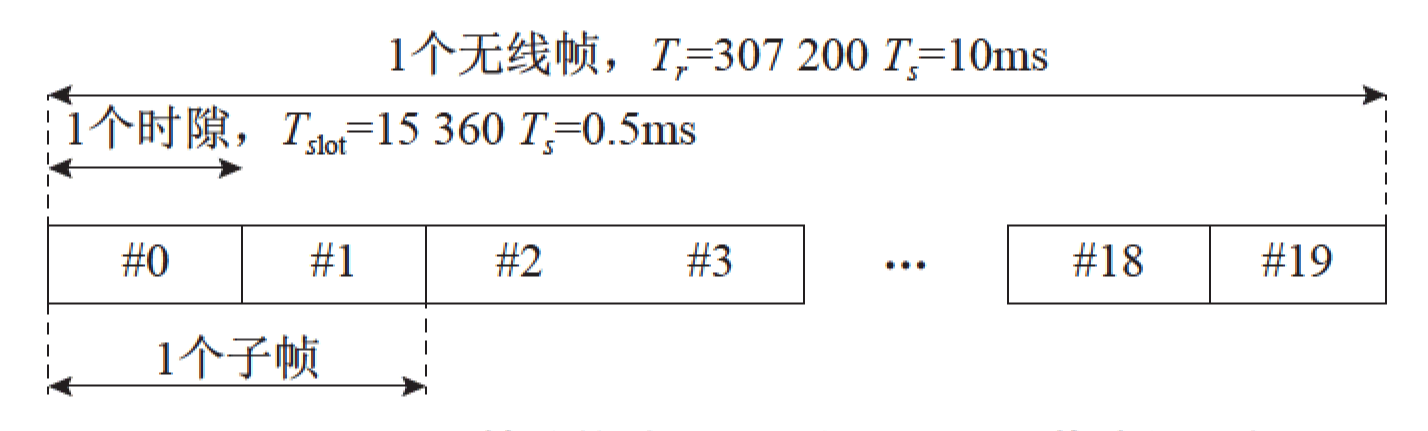


图8-2　NB-IoT帧结构（上、下行15kHz子载波间隔）

上行传输对 15kHz 子载波间隔支持FS1，另外对3.75kHz子载波间隔定义了一种新的帧结构，如图8-3所示。

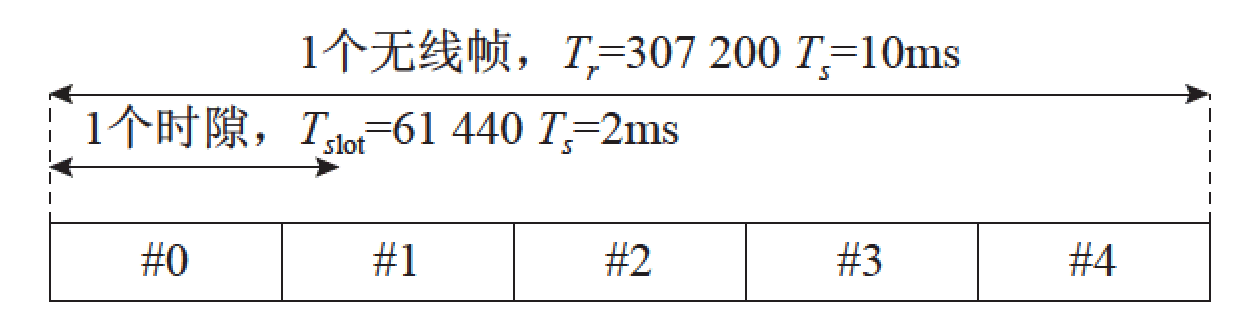


图8-3　NB-IoT帧结构（上行3.75kHz子载波间隔）

3. 关键技术

（1）MIMO技术

NB-IoT下行传输支持两种MIMO模式，单天线端口传输和2天线端口开环发射分集，上行则只支持单天线端口MIMO模式。

（2）半静态链路自适应

NB-IoT的目标业务场景绝大部分为小分组传输，一般没有条件提供长时间、连续的信道质量变化指示，因此，NB-IoT没有设计动态链路自适应方案，而是通过设计三种覆盖等级，根据终端所处的覆盖等级选取数据传输的调制、编码方式及重复次数实现了半静态链路自适应。

三种覆盖等级即常规覆盖（Normal Coverage）、增强覆盖（Robust Coverage）、和极远

覆盖（Extreme Coverage），分别对应链路损耗（Minimum Coupling Loss，MCL）144dB、154dB和164dB，如图8-4所示。NB-IoT基站支持配置1个RSRP 列表，包含两个RSRP门限值，用于区分不同覆盖等级。

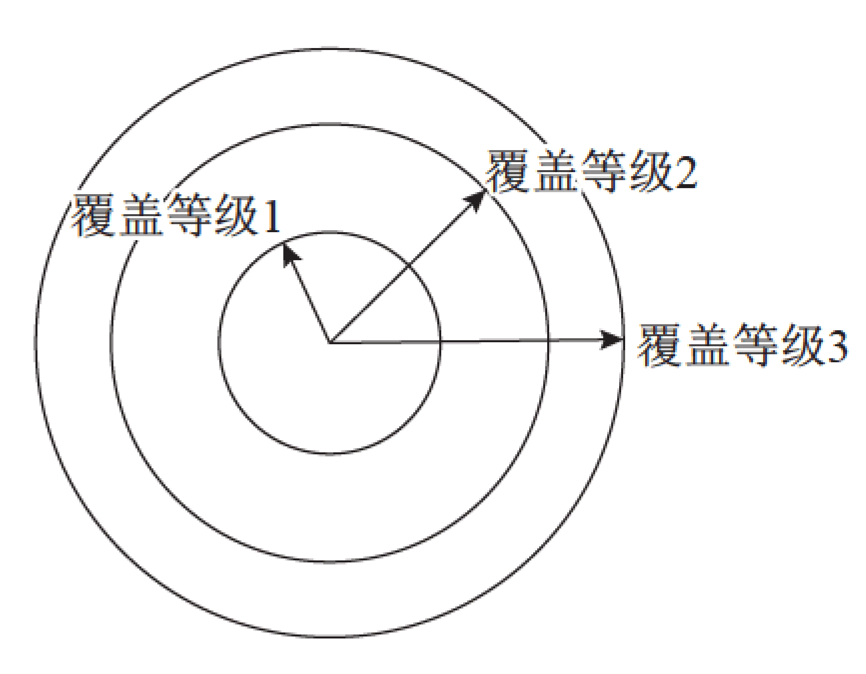


图8-4　NB-IoT的三种覆盖等级

（3）数据重传

NB-IoT采用数据重复发送的方式获得时间分集增益，采用低阶调制方式提高解调性能，增强覆盖性能，各信道均可实现重复发送，且3GPP规定了各信道支持的重复传输次数及对应的调制方式，如表8-1所示。

表8-1　各信道可支持的重复传输次数

项目	物理信号/物理信道名称	重复次数	调制方式
下行	NPBCH（窄带物理广播信道）	固定64次	QPSK
	NPDCCH（窄带物理下行控制信道）	{1,2,4,8,32,64,128,256,512,1 024,2 048}	QPSK
	NPDSCH（窄带物理下行共享信道）	{1,2,4,8,32,64,128,192,256,384,512,768,1 024,1 536,2 048}	QPSK
上行	NPRACH（窄带物理随机接入信道）	{1,2,4,8,32,64,128}	
	NPUSCH（窄带物理上行共享信道）	{1,2,4,8,32,64,128}	ST：π/4-QPSK和π/2-BPSK MT：QPSK

（4）窄带收发技术

获得更高的功率谱密度PSD增益，对比LTE上行3.75kHz，增益为17dB。上行15kHz增益10.8dB。对比GSM上行3.75kHz，增益为7dB，上行15kHz增益为0.8dB，如表8-2所示。

表8-2　各信道可支持的重复传输次数

项目	方　　向	GSM	NB-IoT独立部署	
下行	发射功率（dBm）	43	43	
	占用带宽（kHz）	180	180	
	功率谱密度（$\text{dBm}\cdot\text{kHz}^{-1}$）	20.4	20.4	
上行	最大发射功率（dBm）	33	23	
	最小占用带宽（kHz）	180	15	3.75
	最大功率谱密度（$\text{dBm}\cdot\text{kHz}^{-1}$）	10.4	11.2	17.3

8.1.3 LoRa

1. 概述

低功耗广域网（Low Power Wide Area Network，LPWAN）技术是一种革命性的物联网无线接入新技术，与WiFi、蓝牙、ZigBee等现有成熟商用的无线技术相比，具有远距离、低功耗、低成本、覆盖容量大等优点，适合于在长距离发送小数据量且使用电池供电方式的物联网终端设备。

LPWAN技术从频谱角度上可分为授权频谱和非授权频谱两种。截至目前，低功耗广域网络大部分部署在非授权频谱，即人们熟悉的ISM频段。一旦基于蜂窝网络的LPWAN技术成熟，授权频谱在未来也会成为LPWAN的选择之一。

LoRa是一种新型的基于1GHz以下频谱的超长距低功耗数据传输技术。LoRa主要面向物联网应用，其接收灵敏度可达-148dBm，与业界其他先进水平的Sub-GHz芯片相比，最高的接收灵敏度改善了20dB以上，确保了网络连接的可靠性。LoRa功耗极低，一节五号电池理论上可供终端设备工作10年以上。同时，LoRa使用线性调频扩频调制技术，既可保持像频移键控（Frequency Shift Keying，FSK）调制相同的低功耗特性，又明显增加了通信距离，提高了网络效率并消除了干扰（不同扩频序列的终端即使使用相同的频率同时发送也不会相互干扰），因此在此基础上研发的集中器/网关能够并行接收并处理多个节点的数据，大大扩展了系统容量。

LoRa作为非授权频谱的一种LPWAN无线技术，相比于其他无线技术（如Sigfox、NWave等），其产业链更为成熟、商业化应用较早。LoRa技术经过Semtech、美国思科、IBM、荷兰KPN电信和韩国SK电信等组成的LoRa Alliance国际组织进行全球推广后，目前已成为新物联网应用和智慧城市发展的重要基础支撑技术。

2. 基本原理

作为LPWAN技术之一，LoRa具备长距离、低功耗、低成本、易于部署、标准化等特点，如表8-3所示。

表8-3　LoRa关键特点和优势

关键特点	优势
157dB链路预算	远距离
距离＞15km	
最小的基础设施成本	易于建设和部署
使用网关/集中器扩展系统容量	
电池寿命＞10年	延长电池寿命
接收电流10mA，休眠电流＜200nA	
免牌照的频段	低成本
基础设施成本低	
节点/终端成本低	

LoRa采用线性扩频调制技术，高达157dB的链路预算使其通信距离可达15km以上（与环境有关），空旷地方甚至更远。相比其他广域低功耗物联网技术（如Sigfox），LoRa终端节点在相同的发射功率下可与网关或集中器通信更长距离。LoRa采用自适应数据速率策略，最大网络优化每一个终端节点的通信数据速率、输出功率、带宽、扩频因子等，使其接收电流低达10mA，休眠电流小于200nA，低功耗使得电池寿命有效延长。LoRa网络工作在非授权的频段，前期的基础建设和运营成本很低，终端模块成本约为5美元。LoRaWAN是联盟针对LoRa终端低功耗和网络设备兼容性定义的标准化规范，主要包含网络的通信协议和系统架构。

LoRaWAN的标准化保证了不同模块、终端、网关、服务器之间的互操作性，方案提供商和电信运营商可以加速采用和部署。

（1）LoRa网络架构机制

现有许多部署好的网络都采用了网状结构，每个单独节点要通过其他节点传递信息，这不仅增加了网络的复杂性，而且缩短了电池寿命。LoRa网络架构是一个典型的星状拓扑结构，当实现长距离连接时，终端节点和网关可直接进行信息交互，有效地减少了网络的复杂性和能量损耗，延长了电池寿命，如图8-5所示。

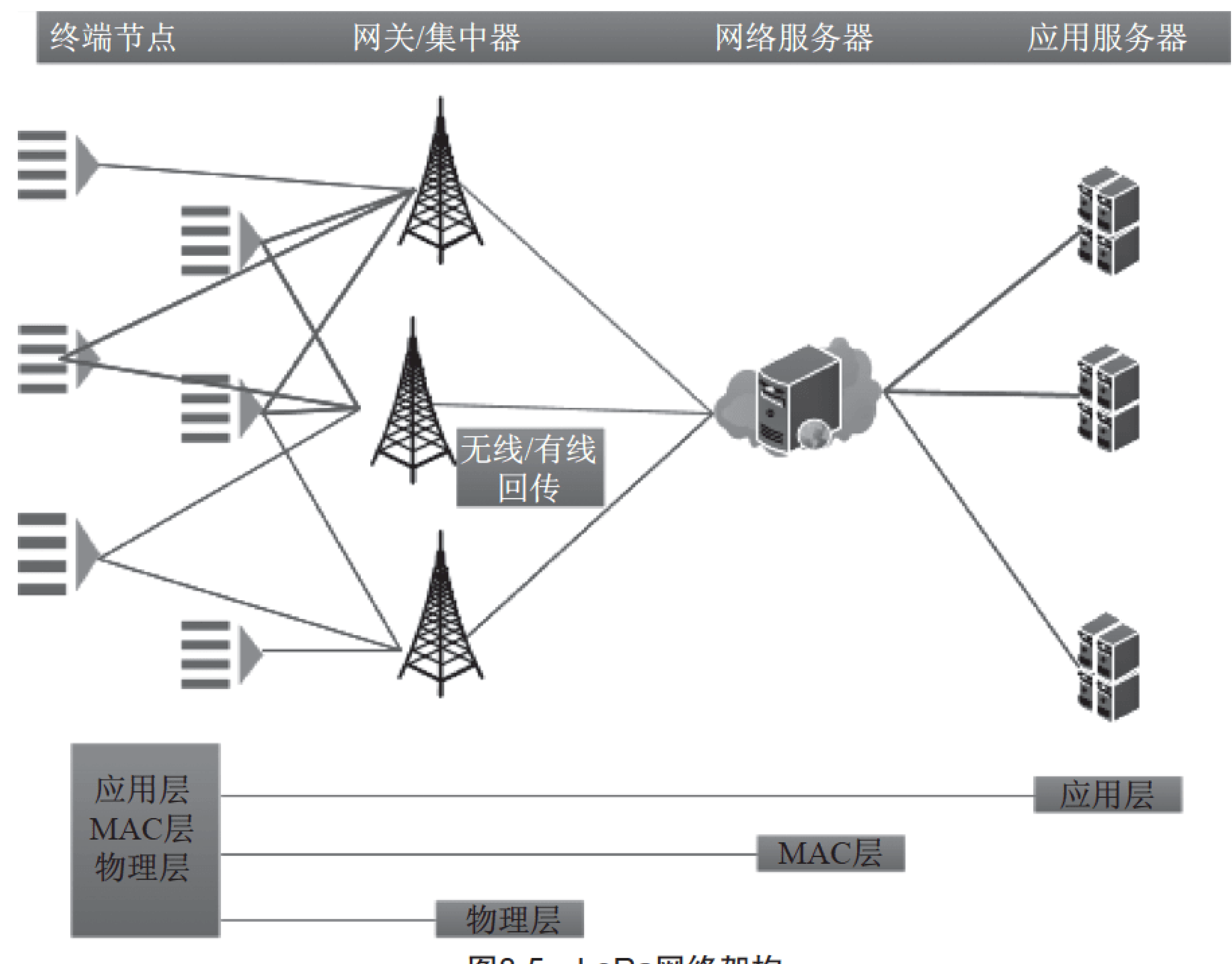


图8-5　LoRa网络架构

LoRa网络架构由终端节点（内置LoRa模块）、网关（或集中器）、网络服务器和应用服务器四部分组成，各组成部分的详细介绍如下：

① 终端节点（含传感器）：包括物理层、MAC层和应用层的实现，使用LoRa线性扩频调制技术，遵守LoRaWAN协议规范，实现点对点远距离传输。

② 网关/集中器：完成空中接口物理层的处理。网关负责接收终端节点的上行链路数据，然后将数据聚集到一个各自单独的回程连接，解决多路数据并发问题，实现数据收集和转发。终端设备采用单跳与一个或多个网关通信，所有的节点均是双向通信。网关和网络服务器通过以太网回传或任何无线通信技术（如2G、3G、4G）建立通信链路，使用标准的TCP/IP连接。

③ 网络服务器：负责进行MAC层处理，包括消除重复的数据包、自适应速率选择、网关管理和选择、进程确认、安全管理等。

④ 应用服务器：从网络服务器获取应用数据，管理数据负载的安全性，分析及利用传感器数据，进行应用状态展示、即时告警等。

（2）终端节点工作模式

LoRa终端有三种不同的工作模式，即Class A、Class B和Class C，一个时间段内终端只能工作于一种模式，每种模式由软件进行设置。不同的模式适用于不同的业务场景和省电模式，目前广泛使用的是Class A类工作模式，以适应IoT应用的省电需求。

Class A（双向终端设备）：A类终端设备提供双向通信，但不能进行主动的下行链路发送。传输时隙由终端设备调度，基于其自身的通信需求并有一个基于随机时基的微小变化，因此A类终端最省电。

Class B（支持下行时隙调度的双向终端设备）：B类终端兼容A类终端，并且支持接收下行Beacon信号来保持与网络的同步，以便在下行调度的时间上进行信息监听，因此功耗会大于A类终端。

Class C（最大接收时隙的双向终端设备）：C类终端仅在发射数据的时刻停止下行接收窗口，适用于大量下行数据的应用。相比于A类和B类终端，C类终端最耗电，但对于服务器到终端的业务，C类模式的时延最小。

3. 关键技术

（1）自适应数据速率（ADR）技术

LoRa网络中的自适应数据速率（Adaptive Data Rate，ADR）是一种改变实际的数据速率以确保可靠的数据包传送，优化网络性能和终端节点容量规模的技术。例如，靠近网关的终端节点使用较高的数据传输速率和较低的输出功率，这样既可缩短传输时间，又可以有效降低功耗。只有在链路预算非常边缘的节点才使用最低的数据速率和最大的输出功率。ADR技术可适应网络基础设施的变化，支持变化的路径损耗。为使终端设备的电池寿命和总体网络容量达到最大化，LoRa网络基础设施（网关、网络服务器）通过ADR实现对每个终端节点的数据速率和RF输出功率进行管理。

在LoRa网络应用条件允许的情况下，建议都对终端节点进行ADR功能设置，具体流程如图8-6所示，这样能延长终端节点的电池寿命。网络对终端节点的数据速率优化调节流程如图8-7所示，其中数据速率的预定策略表由终端节点针对不同应用环境而制定，具体可通过软件实现。

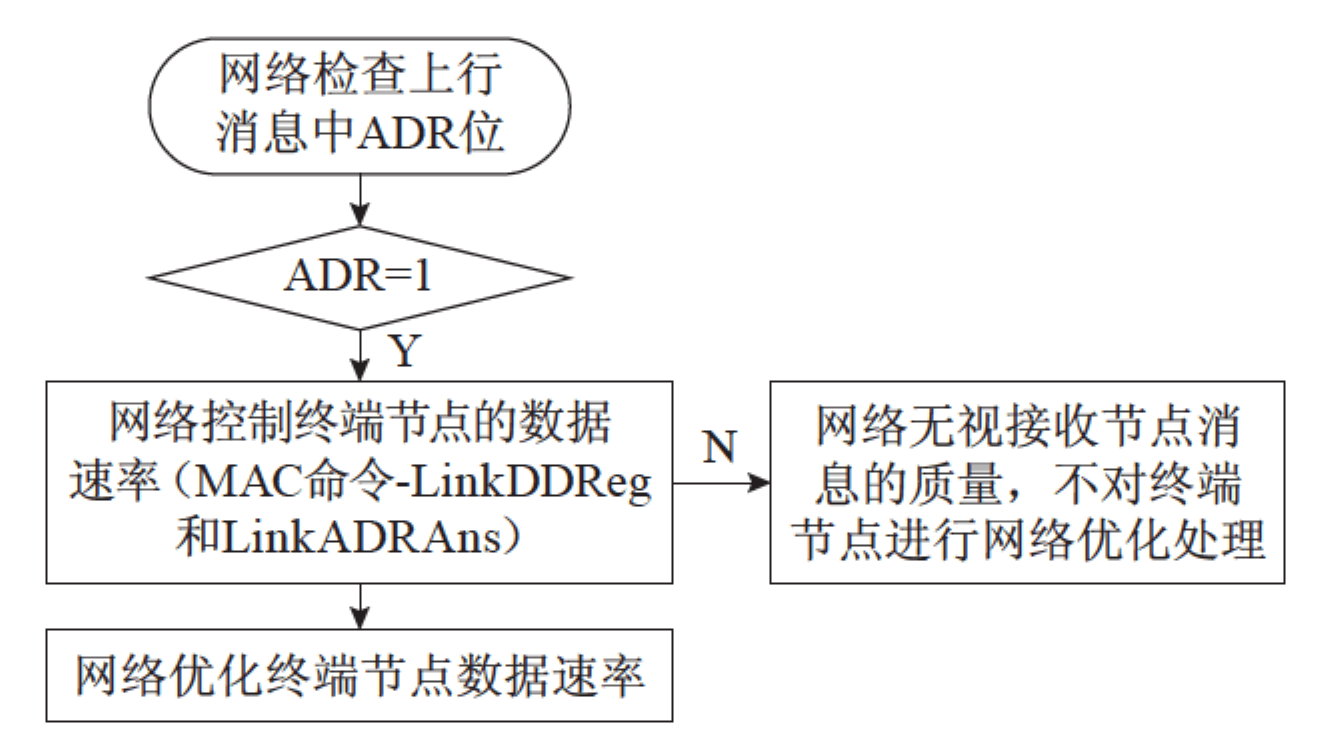


图8-6　LoRa终端节点设置ADR

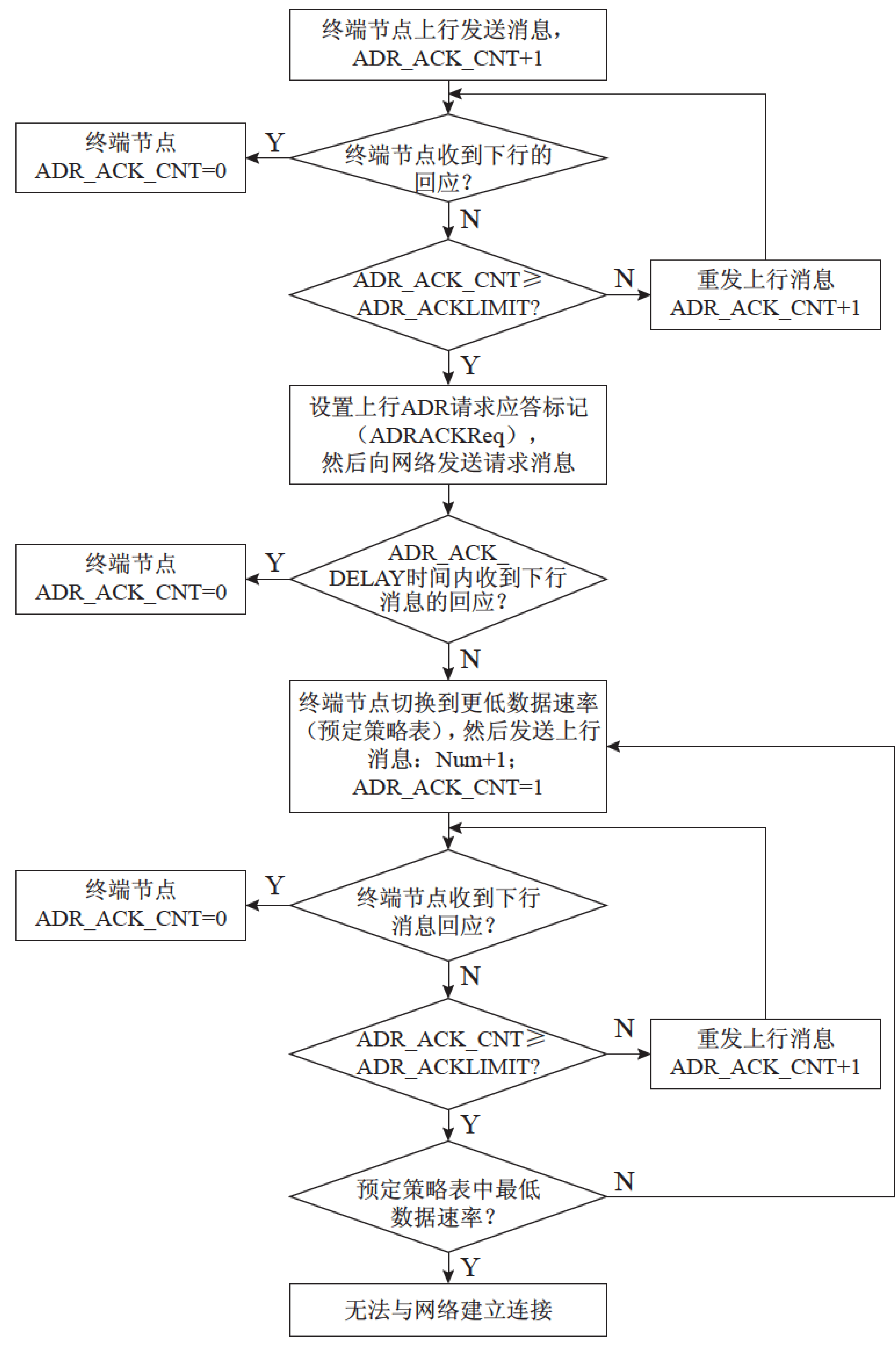


图8-7　自适应数据速率（ADR）调节流程

（2）消息安全加密技术

终端节点必须在与网络服务器消息交互前的一个加入过程完成网络安全的密钥获取。终端节点在接入使用时需具备以下安全信息：终端设备标识（DevEUI）、应用标识（AppEUI）和AES-128应用密钥（AppKey）。其中，DevEUI是唯一标识终端设备的全球终端设备ID，符合IEEE EUI64；AppEUI是存储在终端设备中的全球唯一应用ID，用于识别终端设备的应用程序提供商（即使用者）；AppKey是一个定义于终端设备的AES-128应用密钥，由该应用程序所有者分配给终端设备，从每一个应用独立的根密钥中推演出来，根密钥由程序提供者知晓并处于应用程序提供者的控制下。

当一个终端节点通过无线激活方式加入LoRa网络时，该节点将基于AES128算法，并使用密钥AppKey衍生出终端节点通信所需的会话密钥NwkSKey和应用密钥AppSKey。其中会话密钥NwkSKey用于网络MAC通信的安全保障，而应用密钥AppSKey用于保障应用的端到端安全。

为了保证LoRa网络传输的安全性，终端节点和服务器消息交互前必须先对消息进行加密处理。LoRa网络消息安全加密流程如图8-8所示。

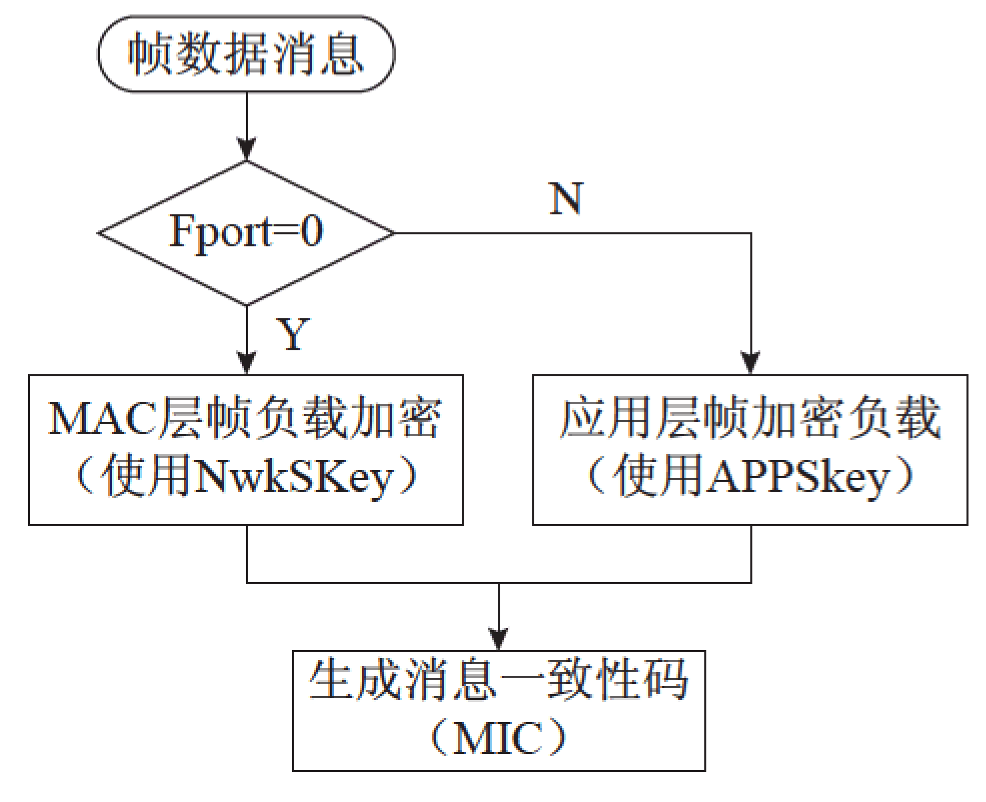


图8-8　消息安全加密流程图

步骤1　使用NwkSKey或AppSKey密钥对MAC负载帧（FRMPayload）加密，其中加密方案使用基于IEEE 802.15.4/2006 Annex B[IEEE 802154]的AES加密，密钥长度为128位。

步骤2　采样基于[RFC4493]：The AES-CMAC Algorithm，June 2006的AES签名算法CMAC生成消息一致性码（MIC），此阶段只使用密钥NwkSKey。其中，当FPort=0时，帧负载只包含MAC命令；而当FPort≠0时，帧负载只包含传输数据，此时FPort值代表帧负载数据的大小。

8.1.4　SigFox

1. 概述

SigFox也是商用化速度较快的一种LPWAN网络技术，它采用超窄带技术，使得网络

设备消耗50μW的功率为双向单向通信或100μW。SigFox采用非授权频段，网络允许很多小型设备接入网络，这些设备往往只需要发送少量数据包的传输数据。

SigFox更像是一个不常联网不常在线的网络，只有在设备需要传输数据时才会连接网络。SigFox 使用的信号频率低于大部分移动数据信号，所以只需要较少的功率就能将数据信号传输到更远的地方。SigFox在空旷地带的覆盖距离可达30～50km，城市内也有3～10km的覆盖范围，可以用很少的基站实现一个区域的网络覆盖。加上SigFox专业网络具有即买即用等优点，诸如物联网、GPS定位追踪器等就很适合使用SigFox。

2. 基本原理

SigFox既是一种无线技术，也是一种网络服务。SigFox工作在868MHz和902MHz的ISM频段，消耗很窄的带宽或功耗。

SigFox无线电设备采用了一种被称为超窄带（UNB）调制的技术。频谱的有效利用通常通过提高M-PSK/M-QAM/M-CPM等典型调制方式的参数达到，此时功率增益往往要随调制状态数的上升而做出相应的牺牲，必须靠编码或者相应编码调制得到一定程度的改进，而这往往以增加复杂性或牺牲时延等其他QoS指标为代价。直接从调制方式入手，大幅改进其功率效率和频谱利用率，采用甚小偏移键控（Very Minimum Shift Keying，VMSK）、甚小波形差键控（Very minimum Waveform Difference Keying，VWDK）等调制方式的UNB技术。它可依据较为简单的概念使频谱利用率得到较大幅度的提高，而同时在未编码状态下即可取得较好的功率增益。

3. 关键技术

Sigfox只面向物联网应用中的短信息类业务，其数据包的大小被限定为12B，这样不仅可以满足类似温湿度、位置等简单信息的传输需求，也限定了单个节点对信道资源的占用时间，使网络可服务更多的节点；在物理层，采用超窄带调制方式，频谱效率高，占用信道资源非常少，网络部署的灵活性也相对较高；在网络架构方面，SigFox采用了跟LoRaWAN类似的简单星状拓扑，终端节点直接与基站进行交互，并且只在有消息推送的时候才会唤醒，传送完毕即进入休眠状态；SigFox还限定了消息的推送次数，上行每天最多140个消息，而下行每天最多4个消息，极大地节省了功耗；SigFox采用固定的传输速率，且仅有100bps，故无须使用复杂的调制方式，核心处理器成本低；核心网也直接部署在云平台上，极大地简化了网络的运营。

总的来说，SigFox将服务定位在短信息类业务，通过限制数据包大小、传输速率、传输频次等并采用简单灵活的组网方式，以获得更好的传输距离和更低的成本。

8.1.5 G

1. 概述

5G作为新一代无线移动通信网络，主要用于满足2020年以后的移动通信需求。在高速发展的移动互联网和不断增长的物联网业务需求共同推动下，要求5G具备低成本、低能耗、安全可靠的特点，同时传输速率提升10到100倍，峰值传输速率达到10Gbps，端到端时延达到毫秒级，连接设备密度增加10～100倍，流量密度提升1000倍，频谱效率提升5～10倍，能够在500 km/h的速度下保证用户体验。5G将使信息通信突破时空限制，给用户带来极佳的交互体验；极大缩短了人与物之间的距离，并快速实现了人与万物的互通互联。

2. 基本原理

5G无线通信技术采用OFDM（正交频分复用）、MC-CDMA（多载波码分多址）、LAS-CDMA（大区域同步码分多址）、UWB（超宽带）、Network-LMDS（区域多点传输服务）和IPv6（互联网协议）。5G网络架构可以分为三大模块：网络部署场景、接入网和核心网。场景部署时室外借住分布式天线（Distributed Antenna System，DAS）和大规模MIMO 配备基站，天线元件分散放置在小区，且通过光纤与基站连接。移动事物（如终端）部署Mo-bile Femtocell，可以动态地改变其到运营商核心网络的连接。同时，部署虚拟蜂窝作为宏蜂窝的补充，提升了室外覆盖率。室内用户只需要与安装在室外建筑的大型天线阵列的室内AP进行通信，就可以利用多种适用于短距离通信的技术实现高速率传输，比如60GHz毫米波通信，可以解决频谱稀缺问题。接入网设计采用异构多接入技术融合，基站资源虚拟化、资源分配集中控制方式，核心网主要由SDN、网络功能虚拟化驱动网络变革。

3. 关键技术

（1）基于滤波器组的多载波技术

在5G系统中，基于滤波器组的多载波技术可以解决频谱效率、对抗多径衰落等方面的问题，FBMC技术是5G系统多载波方案的重要方式。由于在FBMC技术中，多载波性能取决于原型滤波器的设计和调制滤波器的设计，为满足特定的频率响应的特性的要求，需要原型滤波器的长度大于子信道的数量，实现起来复杂且难度高，不利于硬件的效用实现，因而发展和5G要求的滤波器组的快速实现算法是FNMC技术的重要内容。

（2）全双工技术

全双工通信技术即同时同频进行的双向通信技术。在无线通信系统中，网络侧和终端

侧有着固有的发射和接收信号自干扰，当前因技术条件限制，无法实现同时同频的双向通信。全双技术在理论上可提高频谱利用率一倍的潜力，可以实现更为灵活的频谱应用，同时因为器件技术和信号处理技术的发展，同时同频的全双工技术将在5G移动通信系统中得到充分挖掘和应用。

（3）大规模的MIMO技术

多天线技术是提高通信系统频普效率和传输速率、可靠性的有效手段，已经充分应用到各种无线通信系统中，例如3G、WLAN等。根据信息理论，天线数量的多少和频谱效率与可靠性有着密切的联系。在大规模MIMO中，基站需要配置数量庞大的天线，这些天线集中配置在一个基站上的优势在于：ⓐ可深度挖掘空间维度资源，提高频谱效率；ⓑ将波束集中在一定范围内，减少干扰；ⓒ可大幅降低发射功率，提高功率效率；ⓓ当天线够大时，其线性编码和检测最优。大规模MIMO在5G中的应用被寄予了厚望，可以预计大规模MIMO技术将成为5G区别于现有系统的核心技术之一。

（4）超密集异构网络技术

未来5G网络正朝着网络多元化、宽带化、综合化、智能化的方向发展。随着各种智能终端的普及，面向2020年及以后，移动数据流量将呈现爆炸式增长。在未来5G网络中，减小小区半径，增加低功率节点数量，是保证未来5G网络支持1000倍流量增长的核心技术之一。因此，超密集异构网络成为未来5G网络提高数据流量的关键技术。

（5）自组织网络技术

传统移动通信网络中，主要依靠人工方式完成网络部署及运维，既耗费大量人力资源又增加运行成本，而且网络优化也不理想。在未来5G网络中，将面临网络的部署、运营及维护的挑战，这主要是由于网络存在各种无线接入技术，且网络节点覆盖能力各不相同，它们之间的关系错综复杂。因此，自组织网络（Self-Organizing Network，SON）的智能化将成为5G网络必不可少的一项关键技术。

（6）内容分发网络技术

在未来5G中，面向大规模用户的音频、视频、图像等业务急剧增长，网络流量的爆炸式增长会极大地影响用户访问互联网的服务质量。如何有效地分发大流量的业务内容，降低用户获取信息的时延，成为网络运营商和内容提供商面临的一大难题。仅仅依靠增加带宽并不能解决问题，它还受到传输中路由阻塞和时延、网站服务器的处理能力等因素的影响，这些问题的出现与用户服务器之间的距离有密切关系。内容分发网络（Content Distributi-on Network，CDN）会对未来5G网络的容量与用户访问具有重要的支撑作用。

8.2 有线专网技术研究

8.2.1 10G PON

1. 概述

10G PON技术是在EPON/GPON网络框架和特点基础上得出的产物，其主要是以点到多点衔接的技术，无源光分配网络由局侧光线路终端、用户侧光网络单元、光分配网络三部分组成。10G PON应用了具备10G效率的OLT以及ONU，站在系统构造的角度来看，和1G PON具有较高的相似性。

2. 基本原理

与原有PON（EPON/GPON）类似，10G PON 也分为10G EPON和10G GPON，10G EPON以IEEE 802.3av标准为基础，最大限度地沿用了以往IEEE 802.3ah中的内容，具有很好的向上兼容性：将802.3ah 标准中上下行带宽扩大到 10Gbps，充分考虑了与1G EPON的兼容性问题，在规定相关物理参数时，保证 10G EPON的光节点（ONU）可以与1G EPON的ONU共存于同一个光配线网络（ODN）中，且该ODN的配置可以不做任何变化，最大限度地保证了运营商前期的投资。

而 10G GPON则以ITU-T G.987协议组为基础，定义了包括总体特征、物理媒质相关子层、传输汇聚子层和管理控制接口等一系列标准，提出上下行非对称和上下行对称10 PON。

3. 关键技术

10G PON技术和产品的成熟有赖于光模块和功率预算、与EPON/GPON 的后向兼容等关键技术的成熟和完善。

1）功率预算

10G EPON需满足PR/PRX30 29dB的功率预算。根据是否与GPON共存于同一ODN，10G GPON规定了29dB和31dB两种功率预算。在用于FTTH时，需满足至少1∶128 以上的大分光比以便在为用户提供高带宽的情况下保证性价比。另外，10G信号的传输损伤更加严重，且在驻地网内布线时由于环境的复杂可能引入更大的弯曲损耗。

目前的10G EPON和10G GPON标准规定均不能很好地满足FTTH下的功率预算。FSAN正在讨论将10G GPON的功率预算提高到35dB，其方案为在发射端或者接收端集成光放大器，以提高发射光功率或者接收灵敏度。考虑到以上的高分光比和复杂环境需求，以及后续可能的波分复用技术的引入，35dB 的功率预算具有更好的应用前景。

10G EPON采用RS（255，223）FEC，10G GPON正在考虑使用RS（248，216）和

RS（248，232）。10G PON 均采用DFB激光器和高性能的接收机以保证传输性能，上行光突发模式接收模块以及对称式系统的上行光突发发射驱动模块技术难度较大，有待进一步成熟。对于非对称系统，10G EPON和10G GPON的下行信号对光模块的要求一致，上行信号所需的光模块种类和结构基本一致，只是10G GPON 2.5G更高速率的实现难度相对较大；对于对称系统，两种技术对光模块的要求趋同。同时，由于10G EPON的同一OLT板卡下可同时接入10G和1G ONU，下行要求可同时发送1490nm和1577nm 波长，上行需支持双速率突发接收，设备研发难度相对较高。总体而言，10G EPON和10G GPON光模块的研发难度基本相当。

2）向后兼容

10G PON系统需具备后向兼容性，以满足EPON和GPON网络的平滑升级，保护既有投资。10G EPON的同一PON口可接入1G和10G ONU，共享ODN。只要有一个用户升级到10G ONU，该PON口下所有用户都会切换到10G PON口上，需要重新配置用户数据，对实际运维工作要求较高。另外，由于1G和10G EPON上行波长冲突，需采用TDMA方式共享1310 波长，影响总带宽的提升。

10G GPON 通过在OLT侧采用WDM方式与 GPON共享ODN，未来WDM模块可集成在OLT中。10G PON口下仅接入10G ONU，上行信号采用1270nm独立波长，对已有的 GPON系统没有影响，无须重新配置用户数据。后向兼容功能关系到波长分配、MPCP 等协议升级、光模块等相关问题，目前均已解决。

8.2.2　WDM PON

1. 概述

从目前来看，PON技术沿着两个方向发展：一个是单波长大带宽趋势，如10 G GPON，另一个是网络向多波长发展，即WDM-PON技术。WDM-PON是一种采用波分复用技术、点对点的无源光网络，即在同一根光纤中，双向采用的波长数目在3个以上，利用波分复用技术实现上行接入，能够以较低的成本提供较大的工作带宽，它是光纤接入技术未来重要的发展方向。

2. 基本原理

WDM-PON系统由三部分组成：OLT、光波长分配网络（Optical Wavelength Distribution Network，OWDN）和ONU。OLT是局端设备，包括光波分复用器/解复用器（OM/OD），一般具有控制、交换、管理等功能。局端的OM/OD在物理上与OLT设备可以是分立的。OWDN是指在位于OLT与ONU之间，实现从OLT到ONU或者从ONU到OLT的按波长分配的光网络。物理链路上包括馈线光纤和无源远端节点（Passive Remote

Node，PRN）。PRN主要包括热不敏感的阵列波导光栅（Athermal Arrayed Waveguide Grating，AAWG），AAWG是波长敏感无源光器件，完成光波长复用、解复用功能。ONU放置在用户终端，是用户侧的光终端设备。下行方向，多个不同的波长$\lambda d1$，…，λdn在局端OM/OD合波后传送到OWDN，按照不同波长分配到各个ONU中；上行方向，不同用户ONU发射不同的光波长$\lambda u1$，…，λun到OWDN中，在OWDN的PRN处合波，然后传送到OLT，完成光信号的上下行传送。其中，下行波长λdn和上行波长λun，可工作在相同波段，也可工作在不同波段。

3. 关键技术

WDM-PON技术的规模商用因其广阔的发展前景而备受关注，要实现这一目标，就目前技术而言，光模块的可互换性尤其是ONU侧光模块的可互换性是首先需要攻克的难题。基于固定波长光源的技术瓶颈在短期内得不到解决，目前 WDM-PON要实现规模商用的关键在于“无色”光源技术。

就现今的技术水平而言，主要有如下三种方式可以用来实现无色ONU：可调激光器、注入锁定FP-LD（法布理-珀罗腔）和波分复用RSOA（反射式的半导体放大器）。这三种方式原理不同，同时也各有优缺点：

① 利用可调节波长激光器：在可调激光器以特定波长工作的情况下，人为利用外界辅助手段对波长进行有效调节，使激光器根据实际需要发射出不同的波长。在调制技术方面，有两种选择，一是采用直接调制，传输速率可达2.5Gbps 以上；二是采用外调制，可以实现以10Gbps的传输速率，覆盖20km以上的范围。此方案的优点在于不需要种子光源且可调激光器的波长可调范围大，最高达到50nm，可以适应不同的客户需求，易于推广；缺点在于需要制定合理的网络协议对系统运作进行规范，并对ONU波长进行有效调控，这样一来，ONU系统的设计更加复杂，且方案整体成本较高。

② 注入锁定FP-LD：FP-LD在无干扰模式下运作时为多纵模输出，此时如果人为从外部注入适当的种子光，锁模就会被激发从而输出与种子光波长相一致的光信号，FP-LD将其输出的工作波长锁住从而使其与种子光源和波分复用/解复用的通道波长相对应。此方案的优点在于整个系统的网络架构相对简单且系统运作过程中无须制冷控制；不足之处在于传输速率低，传输距离短且成本较高。因为锁模器件FP-LD调制速率低（理论带宽为0.2～4GHz），并且工作过程中器件模间摩擦噪声大，因此无法实现高速率的传输。另外，此系统的运作需要两个种子光源，若用在混合PON中，由于上行信号相比较于下行信号，对种子光源有更高的要求，所以需要高功率的种子光源支持，但其安全性存在问题。这一安全性问题使此系统的传输距离无法超过20km，而导致其无法更好地向外扩展。

③ 波分复RSOA：对种子光源进行频谱分割后将其注入局端RSOA内，RSOA被种子光源激发而输出与种子光波长相一致的光信号。当其作为上行信号的种子光时，就可以激

发ONU内的RSOA输出与种子光波长相一致的光信号，从而实现无色ONU。与注入锁定FP-LD方案类似，此方案系统运作过程中也无须制冷控制，网络架构简单且成本较低；不足之处在于传输距离受限，需要种子光源支持且后向反射较强。

8.3　电力线载波通信技术研究

1. 概述

电力线载波（Power Line Carrier，PLC）是以电力线为信道，以变电站、发电厂为终端的通信方式。在众多通信方式中，电力线载波通信作为专门的通信方式被广泛应用在电力系统中。近年来，随着扩频技术的发展及推广，信号传输的可靠性、抗干扰性、速率得到不断提升。

目前宽带载波通信速率在1Mbps 以上，能够满足智能电网传输数据的要求。电力线载波通信由于不需重新布线，无须进行额外的基础建设和设备维护，且电力线不受恶劣环境的影响。因此，其应用方便、成本经济、信道安全。近几年电力线载波通信在大力发展选频、中继、扩频及自适应调制技术，来满足电力通信网络系统在电力的调度与分配、继电器保护、信息传输等方面的要求。在由传统的电力系统网络向智能电网改造过程中，电力线载波通信必将有非常特殊的重要作用。

2. 基本原理

PLC 通信是利用高压电力线（通常指35kV 及以上电压等级）、中压电力线（指10 kV电压等级）或低压配电线（380/220V用户线）作为信息传输媒介进行语音或数据传输的一种特殊通信方式。电力线载波通信分为传统的频带传输技术和目前流行的扩频通信技术（Spread Spectrum Communication，SSC）。频带传输技术采用载波调制的方法将携带信息的数字信号的频谱搬移到较高的载波频率上。其基本的调制方式分为幅值键控（ASK）、频率键控（FSK）和相位键控（PSK），以及相关派生出的调制技术。扩展频谱通信也叫扩频通信，其信号所占有的频带宽度远大于所传信息必需的最小带宽。频带的展宽是通过编码及调制的方法来实现的，且与所传信息无关。在接收端则用相同的扩频码进行相关运算来解扩及恢复所传信息。

3. 关键技术

1）传统的频带通信技术

传统的频带通信方式价格低廉并且较易实现，所以以往应用比较多。但频带传输技术

的缺点是抗干扰能力较差，尽管频带通信中的接收器具有相对较窄的通带，使得仅有一小部分噪声能进入接收器，但由于此类接收装置中的滤波器具有高品质因数，瞬间的脉冲噪声会使其发生自干扰，引起它对传输来的信号产生误操作；而使用低品质因数的滤波器又会使通带带宽加大，令更多的噪声进入接收器，所以频带通信对脉冲噪声的抵抗性较差。

2）直序扩频通信技术

扩展频谱技术利用高速率的扩频码来达到扩展待传输的数字信息带宽的目的，扩频通信系统的带宽比常规通信机制大几百倍至几千倍，故在相同的信噪比的条件下，具有较强的抗噪声干扰的能力。

3）正交频分复用（OFDM）技术

将输入信息转换成多路并行信号，对相互完全正交的一组载波进行调制。因此OFDM技术的实质是将时分多路（TDM）的数据传输转化为频分多路（FDM）的数据传输。由于各载波之间的正交性，完全消除了彼此之间的串扰，同时可以在接收端利用相同的正交载波组来恢复原始信号。利用OFDM本身的并行正交调制特性，可以有效地抑制电力线上的脉冲噪声和窄带噪声。

4）跳频技术（FH）

跳频是一种无线通信中最常用的扩频方式。其工作原理是收发双方传输信号的载波频率按照预定规律（一组伪随机码）进行离散变化，通信中使用的载波频率受伪随机码的控制而随机跳变。从通信技术的实现方式来说，跳频是一种用码序列进行多频频移键控的通信方式；从时域上来看，跳频信号是一个多频率的频移键控信号；从频域上来看，跳频信号是一个在很宽频带上以不等间隔随机跳变的信号。因此，跳频通信在某一特定频点上仍为普通调制技术。跳频系统根据频率变化的快慢，通常分为快跳频和慢跳频。目前在军事领域广泛应用了快跳频通信技术。随着电子对抗的加剧，在快跳频的基础上，产生了自适应跳频，进一步提高抗截获和抗干扰目的。慢跳频则主要应用于民用领域。

8.4 卫星通信技术研究

8.4.1 北斗技术

1. 概述

北斗卫星导航系统（BeiDou（COMPASS）Navigation Satellite System）是中国正在实施的自主发展、独立运行的全球卫星导航系统。该系统的建设目标是：建成独立自主、开放

兼容、技术先进、稳定可靠的覆盖全球的北斗卫星导航系统，促进卫星导航产业链形成，形成完善的国家卫星导航应用产业支撑、推广和保障体系，推动卫星导航在国民经济社会各行业的广泛应用。

北斗卫星短报文通信具有用户机与用户机、用户机与地面控制中心间双向数字报文通信功能，一般的用户机可一次可传输36个汉字，申请核准的可以达到传送120个汉字或240个代码。短报文不仅可点对点双向通信，而且其提供的指挥端机可进行一点对多点的广播传输，为各种平台应用提供了极大便利。

北斗系统具有全天候、全方位、并发处理能力强、安全性好等特点，表现在：覆盖范围广，目前已覆盖整个亚太地区；系统空间段工作于L/S波段，受强降雨、雪、雾等恶劣天气影响而引起的信号衰减效应非常小，基本能够满足全天候的工作需求；北斗终端设备采用集成化、模块化设计，体积小、功耗低，其天线为全向天线，可在任一方向对星工作；系统的定位、通信与授时使用同一信道，报文数据包为可变长度数据帧，可有效满足通信信息量较小但短时突发数据处理要求较高，且大量用户同时使用的各类应用需求；北斗系统具有良好的加密功能，可保证用户数据通信安全。

所有北斗通信终端都具有唯一标识的用户身份识别卡号，即北斗IC卡号。该卡号由北斗通信网络管理权利机构发出，卡号对应北斗用户的通信级别，每台通信终端的通信频度和通信容量由用户通信级别确定。

2. 基本原理

北斗卫星导航系统由空间段、地面段和用户段三部分组成，空间段包括5颗静止轨道卫星和30颗非静止轨道卫星，地面段包括主控站、注入站和监测站等若干个地面站，用户段包括北斗用户终端以及与其他卫星导航系统兼容的终端。

在北斗卫星导航系统中，能使用无源时间测距技术为全球提供无线电卫星导航服务（RNSS），同时也保留了试验系统中的有源时间测距技术，即提供无线电卫星测定服务（RDSS），但仅在亚太地区实现。从卫星功能来区分，可以分成下列两类：

非静止轨道卫星：北斗卫星导航系统中地球轨道卫星和倾斜地球同步轨道卫星使用东方红三号通信卫星平台并略有改进，有效载荷都为RNSS载荷。

静止轨道卫星：这类卫星使用改进型东方红三号平台，其五颗卫星的定点位置为东经58.75°到160°之间，每颗卫星均有3种有效载荷，即用作有源定位的RDSS载荷、用作无源定位的RNSS载荷、用于客户端间短报文服务的通信载荷。由于此类卫星仅定点在亚太地区上空，故需要用到RDSS载荷的有源定位服务以及用到通信载荷的短报文服务只能在亚太地区提供。

北斗卫星导航系统同时使用静止轨道与非静止轨道卫星，对于亚太范围内的区域导航来说，无须借助中地球轨道卫星，只依靠北斗的地球静止轨道卫星和倾斜地球同步轨道卫星即可保证服务性能。而数量庞大的中地球轨道卫星，主要服务于全球卫星导航系统。此

外，如果倾斜地球同步轨道卫星发生故障，则中地球轨道卫星可以调整轨道予以接替，即作为备份星。

1）北斗通信申请的信道的分析

通信申请的用户机端通过“北斗”卫星与其他的用户机建立通信申请的链接，类似互联网通信的链路层，只不过北斗通信是通过卫星无线互连。“卫星TCP/IP传输技术”中定义的链路层不仅仅指整个系统的通信链接，而是在其基础上高了一个层次。“北斗”卫星通信的实际链路中并没有实现链路控制功能，类似于互联网的物理层。可以类比，数据丢包率类似链路的差错率，通信频度类似于传播延时，信息往返同样也存在信道的不对称性。

2）通信频度和通信量的限制

根据北斗卡的不同级别，北斗卡可以支持的报文通信分为两个级别，普通用户通信频率为120汉字/次；三级北斗卡发送短报文时间频率为 1min一次。

3）数据格式的种类

根据需要，可以选择北斗通信申请的短报文两种数据类型，一种是通常汉字通信采用的ASCII码方式，另一种为BCD码方式。

4）其他通信过程中的干扰因素和制约因素

北斗短报文通信除了易受天气等环境因素的影响，以及数据传输误码率比较大之外，发送短报文的长度和频率也影响了其民用的灵活性，但其对于救援和救急还是起到了较好的补充和保障作用。

3. 关键技术

1）北斗定位技术

卫星定位和卫星导航是不同的概念，通常用RDSS（Radio-Determination Satellite Service）和RNSS（Radio Navigation Satellite System）表示，即卫星无线电测定业务和卫星无线电导航系统，主要区别在于能否完整确定用户位置矢量。北斗系统的定位方式包括有源定位和无源定位。

有源定位是用户需要和地面控制中心联系，采用应答式机制，通过控制中心测量卫星与用户间的距离，并由控制中心确定用户位置，属于一种非自主式定位或被动式定位；北斗系统有源定位采用三球交汇测量原理，即分别以两颗同步卫星为球心，以卫星到用户接收天线距离为半径构成两个球面；两球面相交可得一圆，该圆垂直于赤道平面；在地球不规则球面的基础上增加用户高程，获得一个“加大”的不规则球面；圆与不规则球相交，得两个点，分别位于南北半球，根据用户在半球取点即为用户机位置。

无源定位是用户接受卫星的导航信号完成对每颗卫星的伪距测量，同时从卫星导航信号中解调出卫星星历，得到卫星位置，最后根据已知的位置和测得的伪距求出用户位置，属于一种自主式定位或主动式定位。北斗系统无源定位采用距离交汇测量原理，用户同时

接收来自三颗卫星的广播信息，并且通过测量时差获得卫星到用户的三个伪距，同时用已知的高度，解算出用户位置信息。在这个测量过程中，不需要控制中心参与用户位置解算，但由于钟差的原因需要用户知道所在位置的高程信息。

2）短报文通信技术

指挥机端可通过串口获取发送到的数据，并通过Java等程序接收并处理数据，以实现各种应用。串口非同步传送，参数定义如下：

① 传输速率为19200bps（默认），可根据用户机具体情况设置其他速率；

② 1bit开始位；

③ 8bit数据位；

④ 1bit停止位；

⑤ 无校验。

北斗用户机发送短报文至用户机一般走卫星通道直接发送。但是如果用户机卡绑定了一张主卡的话，子卡的用户机发出的短报文将会往主卡的指挥机发一份短报文。此时，主卡的指挥机将具有广播的功能，可以向与其绑定的所有子卡广播短报文，类似于短信群发功能。此功能可应用在海洋船舶系统中的天气播报、紧急通知等。

由于北斗卡的级别限制，北斗短报文将有1min或30s才能发送一条短报文的限制。一般用户机内将会以队列的方法控制短报文按顺序一条条的发送。但是指挥机端或用户机接收端的接收短报文无时间限制。

北斗用户机向普通手机发送短信，需要经过指挥机端的通信服务进行转发。其原理为：北斗用户机发送短报文至指挥机，指挥机端的通信服务功能通过串口收到短报文。判断短报文内容的前11位为手机号码时，北斗指挥机端基于Java通信服务通过识别手机号，将其短报文通过网络推送至短信网关，再由短信网关发至目标手机，以实现无信号无网络覆盖地的北斗用户机可与普通手机之间的短报文通信功能。相反，普通手机也可以向北斗用户机发送短报文。指挥机端的通信服务收到来自手机的短信之后，通过识别短信内容的前6位判断其发送目标，通过调用指挥机端的接口，采用指挥机发送至用户，达到普通手机发送短信至用户机的目的。

北斗用户机与网站平台或者手机APP互发短报文。这是在用户机和普通手机通信的基础上封装得比较友好的应用，以满足使用者的操作。

北斗短报文功能提供了紧急通道，此通道无时间限制，可以按照设定的时间间隔不断发出求救信息。但是此求救信息会消耗普通短报文的时间。例如，正常发送一条短报文，它与发送的前一报文时间间隔是1min，如果连续发送5条紧急求救信息，将消耗用户机5min的时间，此5min内用户机将无法发出任何短报文。一般紧急救援的短报文发送提供设备按钮或者软件按钮，以最简便快捷的方式提供给用户，以便在紧急情况下使用。

3）授时授频技术

现阶段GPS的授时功能在电力系统中的应用是重要和普遍的。电力系统中如微机监控

系统、故障录波器、事故记录仪等许多自动化装置采用的时间源都来自于GPS系统。GPS系统作为精度最高的时间发布系统之一，其最高精度可达20ns。

北斗导航系统具有单向和双向两种授时功能，根据不同的精度要求，利用设定时间和频率同步，提供单向授时100ns和双向授时20ns的时间同步精度。

在单向授时模式下，用户机不需要与地面中心站进行交互，但需已知接收机精密坐标，从而计算出卫星信号传输时延，经修正得出本地精确的时间。中心控制站精确保持标准北斗时间，并定时播发授时信息，为定时用户提供时延修正值。标准时间信息经过中心站到卫星的上行传输延时、卫星到用户机的下行时延以及其他各种时延传送到用户机，用户机通过接收导航电文及相关信息自主计算出时钟差并修正本地时间，使本地时间和北斗时间同步，系统设计授时指标为100ns。

双向定时的所有信息处理都在中心控制站进行，用户机只需把接收的时标信号返回即可。中心站系统在$T0$时刻发送时标信号$ST0$，该时标信号经过时延$\tau 1$后到达卫星，经卫星转发器转发后经$\tau 2$到达定时用户机，用户机对接收到的信号进行处理，也可看作信号转发，经$\tau 3$的传播时延到达卫星，卫星把接收到的信号进行转发，经$\tau 4$的传播时延传送回中心站系统。也即表示时间$T0$的时标信号$ST0$，最终在$T0+\tau 1+\tau 2+\tau 3+\tau 4$时刻重新回到中心站系统。中心站系统将接收时标信号的时间与发射时刻相减，得到双向传播时延$\tau 1+\tau 2+\tau 3+\tau 4$，再除以2得到从中心站到用户机的单向传播时延。中心站把这个单向传播时延发送给用户机，定时用户机接收到的时标信号及单向传播时延计算出本地时钟与中心控制系统时间的差值$\Delta\varepsilon$，修正本地时钟，使之与中心控制系统的时间同步。

8.4.2 宽带卫星通信

1. 概述

宽带卫星通信系统已成为当前通信发展的热点之一。先前的卫星宽带系统被称为卫星宽带接入系统。为了提供更高的带宽，现代宽带多媒体卫星通信系统都倾向于工作在更高的频段，其关键技术与已经出现的第三代地面通信系统（3G）相同，都是利用IP和IP/ATM提供高速、直接的因特网接入和各种多媒体信息服务。由于多媒体业务普遍需要服务质量（QoS）保证，卫星ATM系统具有很光明的应用前景，在保证各类业务QoS的同时，能灵活、高效、合理地将系统资源分配给各种类型的业务连接，达到卫星信道的最佳分配利用。

研究人员已将4G（第四代）通信系统当作一个涵盖了卫星和地面领域的统一实体来看。将IP/ATM与卫星技术相结合的宽带卫星通信网具有地面覆盖面广、承载业务种类多、可快速部署、带宽利用率较高、星上交换快捷、可提供一体化网络等特点，能满足不同用户的业务需求。它既可以用作专用通信网，也可以作为公共通信网的一部分。同时，它还能

起到将若干远距离地域分布的地面宽带通信网络连接在一起的宽带信息技术桥梁的作用。

2. 基本原理

目前国际上已经出现的已发射及待发射的宽带卫星系统有10多个，采用的技术多种多样，依轨道的不同有地球同步静止轨道（GEO）、中轨道（MEO）、低轨道（LEO），甚至混合轨道之分，卫星系统由单一卫星直至几百颗卫星的星座构成。

1）静止轨道通信卫星星座系统

静止轨道（GEO）卫星位于赤道平面，使用3颗卫星就可接近实现全球覆盖，但由于卫星的轨道高度较高，路径损耗较大，信号有较大时延，单跳传输时延为250~280ms，对话音和视频传输有较高要求。

2）中轨道/低轨道卫星星座系统

中轨道（MEO）、低轨道（LEO）通信卫星的信号传输时延分别只有110～130ms、20～23ms，可在任何两个用户之间提供近似实时交互式业务。然而若要达到全球覆盖，MEO及LEO卫星星座所需卫星数量将会很多。MEO /LEO卫星系统控制和网络管理比较复杂，其好处是通过大批量的生产和发射可以降低单颗卫星的造价和发射费用，但随着卫星数量的增加，系统总体投资规模也会加大。

3）静止轨道和非静止轨道卫星的混合星座

将 GEO和 LEO的各自优点结合使用出现了混合星座。GEO与LEO相比其突出优势是覆盖范围广阔，适于进行广播和组播业务。然而长时延使得GEO卫星明显不如LEO更适合于话音和交互视频业务，而且LEO可降低终端功耗，且可使接收终端天线更小。

3. 关键技术

IP、ATM或两者的结合（如IP/ATM）被视为是能有效构成未来多媒体信息骨干网的关键技术。ATM被设计用来支持具有QoS保证的各类业务；而IP目前只支持单一QoS保证的“尽力而为”（best effort）传递业务，预计未来能支持多个 QoS类别及多媒体业务。

1）卫星ATM网络

采用基于ATM 技术的具有复杂的星上处理（OBP）、星上交换（OBS）和星上路由（OBR）技术可将信息从一条上行链路点波束直接路由到指定下行链路点波束，与传统的采用透明弯管式（bentpipe）转发中继器的卫星系统结构相比，可以将传送时间减半。

具有OBP功能、上行链路采用多频时分多址（MF-TDMA）接入技术，下行链路采用时分复用（TDM）技术、工作在Ka频段的多点波束的地球同步静止轨道（GEO）卫星系统，由若干束下行链路点波束覆盖地球表面。分布于地面各处的用户根据其地理位置的不同使用几条上行链路点波束中的一条接入到卫星，这些用户可以是使用语音、视频或数据的用户。每个用户必须与在同一点波束内的其他用户共享带宽资源。

具有OBP功能的Ka频段卫星载荷包含业务资源管理器（TRM），负责资源分配和交换

配置；网关地面站（GTW）互联卫星和地面网；不同类型的卫星用户终端（UT）用于接入到系统；主控站（MCS）负责对整个系统的监控。

2）波束成形技术

卫星上装有两种天线，一种是遥测、指令信标天线，一般是全向天线，以便可靠地接收指令并向地面发射遥测数据和信标；另一种是通信天线，根据需要可设计成全球波束天线、区域波束或点波束天线、赋形波束天线。

全球波束天线：对于静止卫星而言，其波束的半功率角宽度为17.44°，恰好覆盖卫星对地球的整个视区。

区域波束或点波束天线：波束半功率角宽度较小，只有几度或更小；使波束只覆盖某一地区，功率比较集中，能更好地满足某一地区的通信要求。更小的波束为特定的小区提供特殊通信服务，称为点波束。

赋形波束天线：波束覆盖轮廓不规则，视服务区的形状而定。为使波束成形，有的技术是通过修改反射器形状来实现，更多的是利用多个馈源从不同方向经反射器产生多波束的组合来实现。还有一种使用简单发射单元的平面阵列实现波束成形技术，该方法的主要优点是波束成形是全数字的，并采用自适应处理技术，增大了设计的自由度。同时平面天线的制造成本相对于抛物面天线低，重量也轻。

3）星上处理技术

传统的弯管（bent pipe）模式卫星系统是由用户站、网络主控制站（MCS）和卫星组成。此时的卫星只作为一个彻底透明的中继转发器，所以必须由MCS控制所有用户间的连接。

卫星系统内的用户必须建立TDMA帧同步和时隙同步。同步确定后，用户通过卫星向MCS发送包括目的地、频率、吞吐量等连接请求（呼叫建立请求）。当MCS收到呼叫请求后，即检查卫星资源，如时隙、发射功率和频道等的可用性。假如资源可供分配，MCS即接受连接请求并为用户分配信道，随后将信道分配结果传递给信源站和信宿站。在此阶段，用户能够向卫星网络注册并获取时隙分配，然后信源站按照分配的时隙与信宿站连接并交换用户数据。当用户想切断或注销连接时，用户只需向MCS发送一个呼叫释放请求，MCS收到该请求后，即解除用户时隙分配。

再生型卫星系统是由用户站、主控制站（MCS）和卫星组成，该模式中星上交换机可以识别用户发送数据的路由信息。

再生模式的接入流程基本与弯管模式的相同，同步和信道联络的建立阶段也相同。然而，在再生模式中，上行链路和下行链路可被视为独立的信道，因为通知信息是由星上ATM 交换机发出，且ATM交换机可以解调上行链路信号并缓存ATM 信元。所以，下行链路帧的首个时隙被用作通知时隙，而上行链路帧的首个时隙被用作联络时隙，两者的剩余时隙被用作数据时隙。

再生模式可以避免上下行噪声积累，提高频谱利用率和等效全向辐射功率（EIRP），

缩小终端尺寸，适应复杂的通信流量变化，有效利用信道资源。

4）星间链路

星间链路（ISL）就是卫星之间的通信链路，在空间上构成了通信子网。开发ISL 网络的主要益处是在使用最少的地面资源的前提下，通过可靠和高容量的星间连接来进行长距离通信。现代卫星由于采用了先进的OBS/OBP技术，具有了ISL通信功能，使用ATM交换技术，意味着在ISL路径上的每个卫星节点均时延较低，加之LEO/MEO上行和下行链路具有较低的传播时延，使其适合于ISL传输。ISL也构成传播时延的一部分，其既可以是存在于同轨道平面内（in-plane）卫星间的同轨道ISL，也可以是存在于不同轨道平面内（cross-plane）卫星间的异轨道ISL。对于GEO 系统，ISL时延可认为是不变的；而LEO系统的ISL时延则要取决于轨道半径、每条轨道内卫星的数量和轨道间的距离。LEO系统的ISL时延会因卫星移动和自适应路由技术而频繁改变，ISL亦可采用微波传输和光波传输技术。

5）切换及路由重建

非GEO卫星沿轨道飞行引发了其与地面终端相对位置的改变，结果是，主控站必须负责将原连接切换至另一颗移入此覆盖区域的卫星上。切换分为同轨道卫星间切换与异轨道卫星间切换。GEO系统因其高轨道覆盖范围广，不存在太多的切换问题； 而LEO卫星平均约8～11min发生一次切换。同时LEO星座因切换会产生较大的时延变化。具有多跳星间链路（ISL）LEO系统需有良好的切换及路由重建协议，以便在卫星切换后仍保持原路由的最佳状态； 处理异轨间的切换问题； 保持ATM信元传递次序。

8.5 通信安全技术

8.5.1 可信计算

1. 概述

信息安全具有四个侧面：设备安全、数据安全、内容安全与行为安全。

可信计算为行为安全而生，行为安全应该包括行为的机密性、行为的完整性、行为的真实性等特征。

从概念上来说，可信计算（Trusted Computing，TC）并非由可信计算组织（Trusted Computing Group，TCG以前称为TCPA）率先提出。可信这个概念早在彩虹系列的橘皮书就已提及，其目标是提出一种能够超越预设安全规则，执行特殊行为的运行实体。操作系

统中将这个实体运行的环境称为可信计算基（Trusted Computing Base，TCB）。

为了实现这个目标，人们从20世纪70年代开始就在不懈地努力，包括从应用程序层面，从操作系统层面，从硬件层面提出的TCB相当多。最为实用的是以硬件平台为基础的可信计算平台（Trusted Computing Platform，TCP），它包括安全协处理器、密码加速器、个人令牌、软件狗、可信平台模块（Trusted Platform Modules，TPM）以及增强型CPU、安全设备和多功能设备。

这些实例的目标是实现数据的真实性、数据的机密性、数据保护以及代码的真实性、代码的机密性和代码的保护。

根据S.W.Smith最近的著作《可信计算平台：设计与应用》（冯登国等翻译，清华大学出版社出版），这些平台的实现目的包括两个层面的意思：保护指定的数据存储区，防止敌手实施特定类型的物理访问；赋予所有在计算平台上执行的代码以证明它在一个未被篡改环境中运行的能力。

从广义的角度，可信计算平台为网络用户提供了一个更为宽广的安全环境，它从安全体系的角度来描述安全问题，确保用户的安全执行环境，突破被动防御的打补丁方式。

2. 基本原理

可信计算技术是指在PC硬件平台引入安全芯片架构，通过其提供的安全特性来提高终端系统的安全性，从而在根本上实现了对各种不安全因素的主动防御。其核心就是在用户与计算机、网络平台间建立一种信任机制。它包括以下5个关键技术概念，它们是完整可信系统所必需的，这个系统将遵从TCG（Trusted Computing Group）规范。

1）签注密钥（endorsement key）

签注密钥是一个2048b的RSA公共和私有密钥对，它在芯片出厂时随机生成并且不能改变。这个私有密钥永远在芯片里，而公共密钥用来认证及加密发送到该芯片的敏感数据。

2）安全输入输出（secure input and output）

安全输入输出是指电脑用户和他们认为与之交互的软件间受保护的路径。当前，电脑系统上恶意软件使用了许多方式来拦截用户和软件进程间传送的数据，例如键盘监听和截屏。

3）储存器屏蔽（memory curtaining）

储存器屏蔽拓展了一般的储存保护技术，提供了完全独立的储存区域，如包含密钥的位置。即使操作系统自身也没有被屏蔽储存的完全访问权限，所以入侵者即便控制了操作系统，信息也是安全的。

4）密封储存（sealed storage）

密封存储通过把私有信息和使用的软硬件平台配置信息捆绑在一起来保护私有信息。这意味着该数据只能在相同的软硬件组合环境下读取。例如，某个用户在他的电脑上保存一首歌曲，而他的电脑没有播放这首歌的许可证，那么他们就不能播放这首歌。

5）远程认证（remote attestation）

远程认证准许用户电脑上的改变被授权方感知，例如软件公司可以避免用户干扰他们的软件以规避技术保护措施。它通过让硬件生成当前软件的证明书，随后电脑将这个证明书传送给远程被授权方来显示该软件公司的软件尚未被干扰（尝试破解）。

可信计算可以从以下几个方面来理解：

① 用户的身份认证：对使用者的信任。

② 平台软硬件配置的正确性：体现使用者对平台运行环境的信任。

③ 应用程序的完整性和合法性：体现了应用程序运行的可信。

④ 平台之间的可验证性：指网络环境下平台之间的相互信任。

可信计算通过在硬件平台上引入安全芯片（可信平台模块）来提高终端系统的安全性，也就是说是在每个终端平台上植入一个信任根，让计算机从BIOS到操作系统内核层，再到应用层都构建信任关系;以此为基础，扩大到网络上，建立相应的信任链，从而进入计算免疫时代。当终端受到攻击时，可实现自我保护、自我管理和自我恢复。

可信计算涉及：可信计算安全芯片，密码技术和密钥体系，PKI/PMI技术，身份、权限管理（包括系统管理员），认证体系，可信接入安全服务平台，以及相应的法律、政策支撑等。

着力打造可信计算平台是信息安全保障的重要使命，通过平台，实现保护指定的数据存储区，防止敌手实施特定类型的物理访问；赋予所有在平台上执行的代码以证明它在一个未被篡改环境中运行的能力；可信计算平台为网络用户提供了一个更为宽广的安全环境，它从安全体系的角度来描述安全问题，确保用户的安全执行环境，突破被动防御打补丁的方式。

3. 关键技术

可信计算涉及的关键技术和热点技术有：在硬件层，主要是TPM的涉及技术；在BIOS层，主要包括CRTM、MA/MP驱动的设计技术；在操作系统上，主要是可信软件栈的设计技术；在应用层上，主要是可信网络连接技术。通过这些关键技术的设计，最终建立可信计算机的信任链传递机制，如图8-9所示。

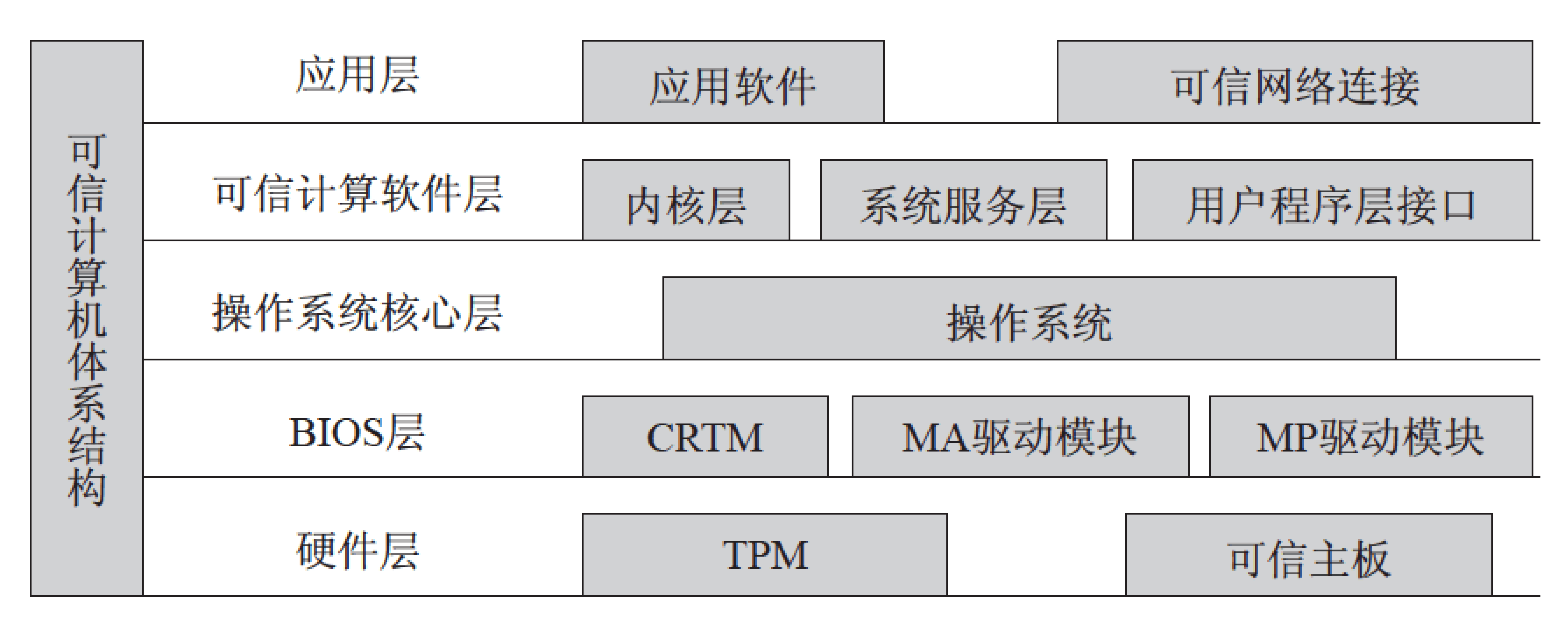


图8-9　可信计算关键技术

1）信任链传递技术

TCG认为如果从一个初始的信任根出发，在计算机终端平台环境的每一次转换时，这种信任状态可以通过传递的方式保持下去且不被破坏，那么表明平台上的计算环境始终是可信的。在可信环境下的各种操作也不会破坏平台的可信，平台本身的完整性得到保证，终端安全也就得到了保证，这就是信任链传递机制。

可信计算机的信任根是由度量信任根核（CRTM，BIOS的一部分）和TPM共同组成的。对平台的信任是基于TPM和CRTM的可信性，信任传递是信任根给出第二组函数的可信性描述，基于这一描述，访问实体来确定对这组函数的信任程度。如果访问实体认为这组函数的可信等级是可以接受的，信任边界就从信任根扩展到包含这组函数。这一过程可以循环进行，第二组函数可以给出第三组的可信性描述，这样就将信任扩展到整个平台，并进一步扩展到网络上的其他平台。信任传递用来提供平台特征的一个可信性描述。

T平台复位时CRTM获得可信构建块（由TPM、CRTM与TPM的连接、TPM与主板的连接构成）的控制权，在传输控制权之前，可信构建块必须对它将要传输给控制权的实体进行度量，这种度量就是对安全计算机完整性一种度量。

图8-10是应用于从一个信任根开始系统引导的信任传递过程。在每次扩展可信边界时，执行控制权移交之前要进行目标代码的度量。通过构建信任链传递机制，各个环境的安全性得以保证，从而使整个平台的安全性得以保证。

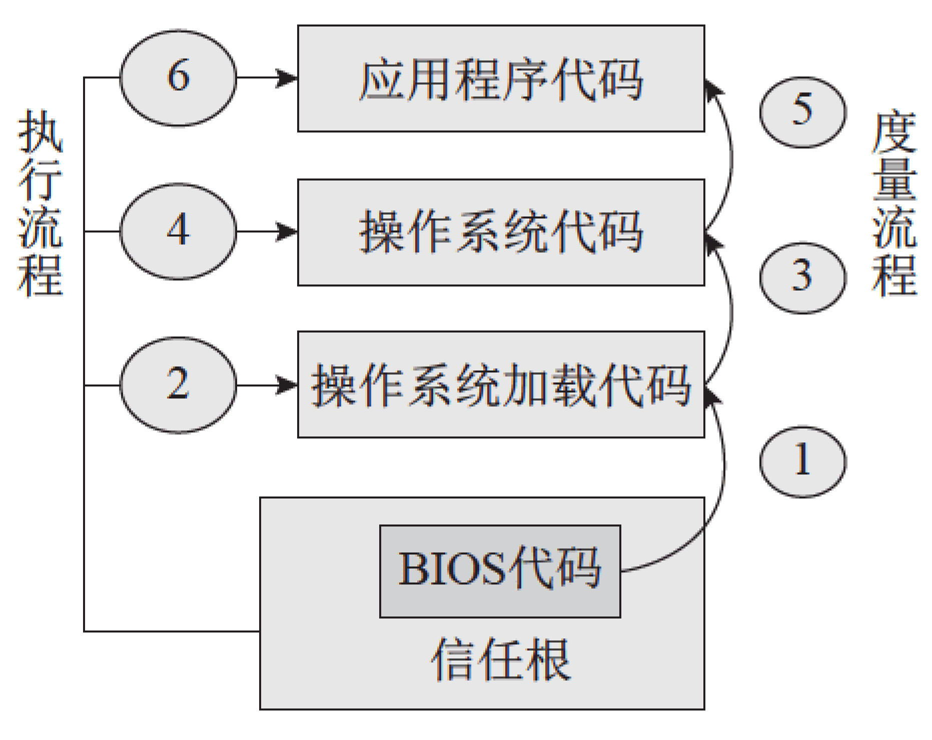


图8-10 信任传递过程

2）信任传递流程

在平台初始化过程中，平台的执行从CRTM开始，CRTM是平台初始化代码中不变的部分，对有度量的信任基于这个组件的完整性，CRTM的执行日志将会被记录到TPM的平台配置寄存器中来验证其完整性。首先CRTM记录其自身版本标识，然后对其传递给控制权的代码进行度量，最后对物理绑定在主板上的固件、ACPI Flash数据、BIS代码的完整性进行度量。如果度量未通过则平台复位；如果度量通过BIOS将进行主板配置信息的度量，主板配置信息包括硬件组件以及它们的配置，此时对ESCD、CMOS、其他NVRAM数据以及用户口令进行度量。如果度量通过将由BIOS对可选ROM代码进行度量，这些可

选ROM物理包含在主板上，并与附加卡相对应，任何应用程序对可选ROM代码做出的修改都必须重新度量，否则平台复位。可选ROM都被度量并执行以后，由可选ROM对与平台安全性相关的配置和数据进行度量，如果度量通过，可选ROM将控制权交还给BIOS，BIOS将对每个初始加载代码进行度量。BIOS完成初始化以及平台硬件测试后将信任传递给操作系统，在这个阶段平台将传递信任根，BIOS会将信任链传递给MBR，然后MBR保存信任链并将信任传递给操作系统，将TPM的控制权移交给操作系统后，操作系统会加载可信计算软件栈来访问TPM，同时关闭BIOS对TPM的支持。这样就完成了开机启动过程中整个信任链的传递，如图8-11所示。

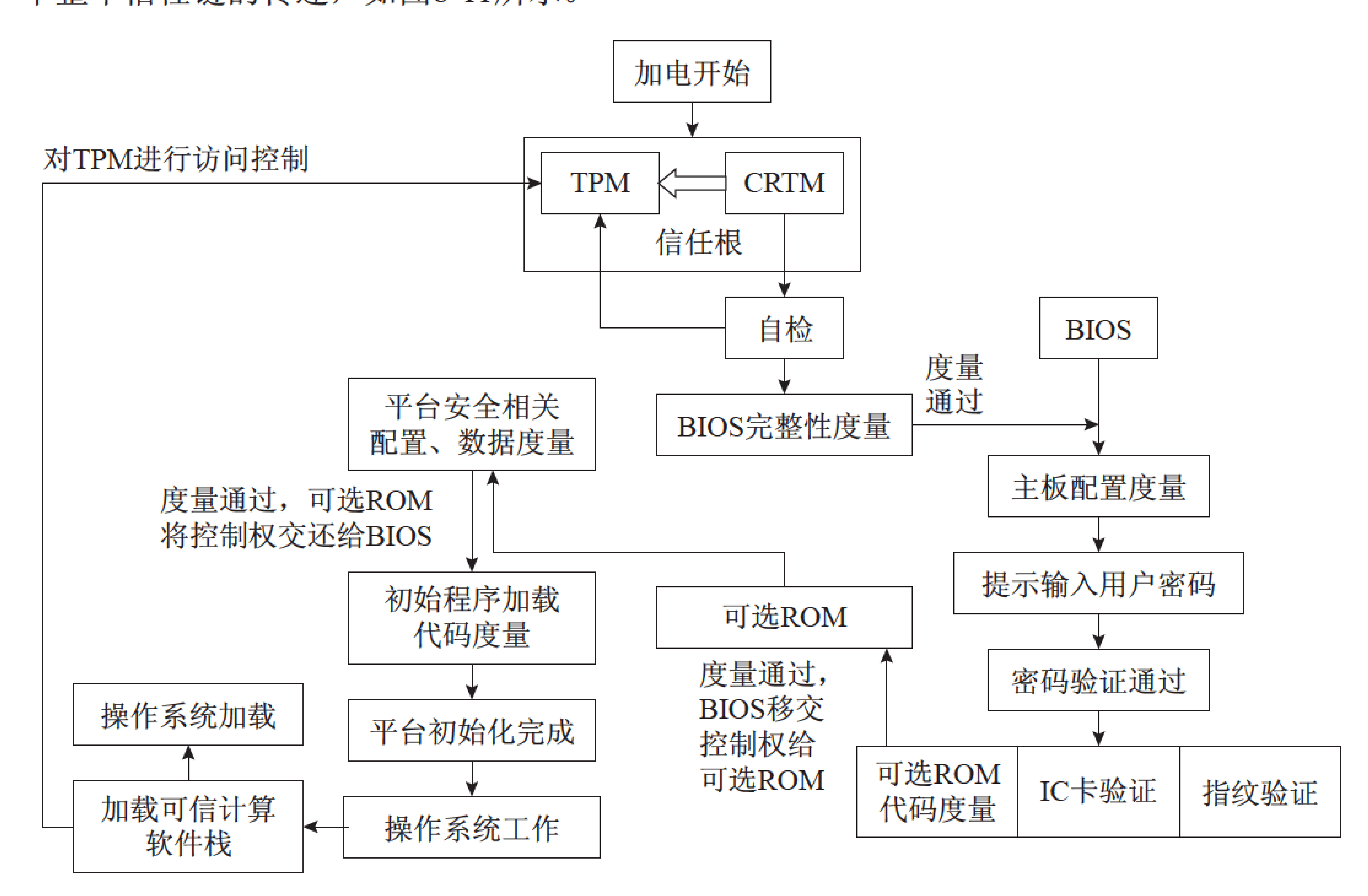


图8-11　信任链传递流程

3）TPM 设计技术

TPM是一个密码芯片硬件装置，它储存了独特的平台信息和加密密钥，并包括了一个用于加密算法的随机数发生器。它为安全可信计算提供硬件保护，能够提供以下主要安全功能。

① 受保护的密码处理过程，包括硬件保护下的密钥生成、随机数生成、Hash和数字签名操作以及加解密操作。

② 受保护的存储，即提供安全封闭式空间来存储信息，对敏感数据进行硬件保护存储。

③ 平台认证。TPM包含一个密码学上唯一的值，这个值只在平台所有者的控制下被用来生成平台别名ID以提供对可信平台身份的认证。

④ 平台可信状态，即具有对平台可信状态证明的通信能力。

⑤ 存储和报告数据完整性测量结果。

⑥ 初始化和管理功能。

TPM的结构如图8-12所示。

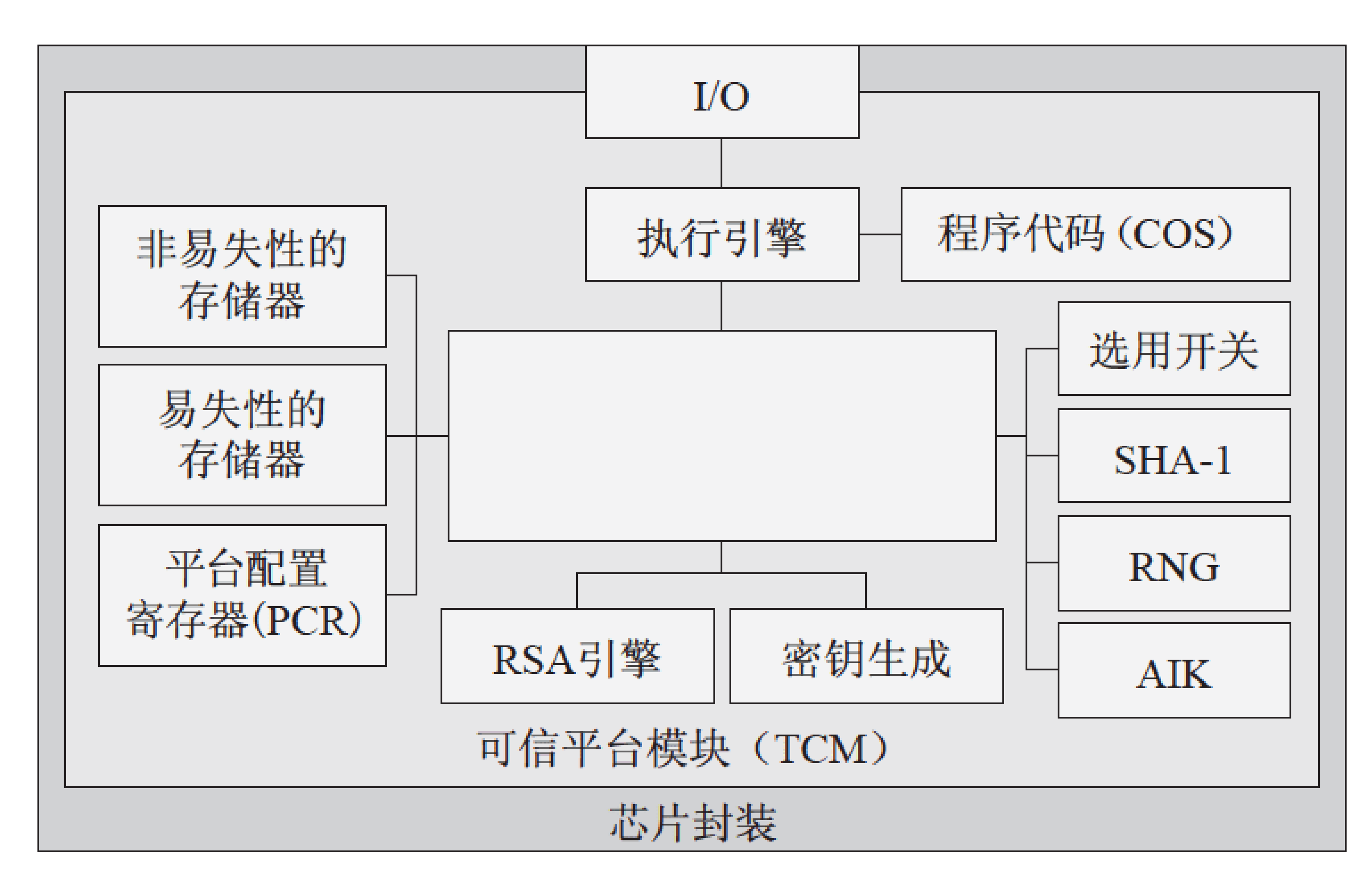


图8-12 TPM的结构

TPM的实现可以在硬件或软件中完成。

4）可信软件栈设计技术

可信计算软件栈由内核层、系统服务层和用户程序层三部分组成，其中内核层的核心软件是可信设备驱动模块，系统服务层的核心软件是可信设备驱动库模块和可信计算服务模块，而用户层的核心软件则是可信服务提供模块。各层次模块的结果和功能如下：

① 可信设备驱动模块：直接驱动TPM的软件模块。

② 可信设备驱动库模块：是可信计算服务模块与运行在核心态的可信设备驱动模块之间的中间模块，其提供的用户模式接口用来完成用户模式和内核模式的转换。该模块向上提供了独立于操作系统的编程接口，可以保证可信计算软件栈中不同的软件实现实体正确地和任意的可信设备进行操作。

③ 可信计算服务模块：对一个平台上的多个可信服务提供模块提供一组通用的服务。

④ 可信服务提供模块：是可信计算软件栈提供给应用程序的最高处API函数，可以向应用程序提供C语言编程接口，负责在应用程序中运行TPM提供的可信运算功能。

在图8-13中，最下层是TPM的硬件装置，它经由TPM设备驱动库来访问。应用程序可以通过加密API（MS-CAPI）标准接口或者是通过直接执行可信软件栈的通信接口来使用TPM。可信计算软件栈为TPM提供支持函数。一些超出了TPM硬件范围的函数和服务通过主CPU和系统内存进行传输。可信计算软件栈提供必要的软件结构来支持从TPM中将安全功能下载到主CPU和系统内存资源中。

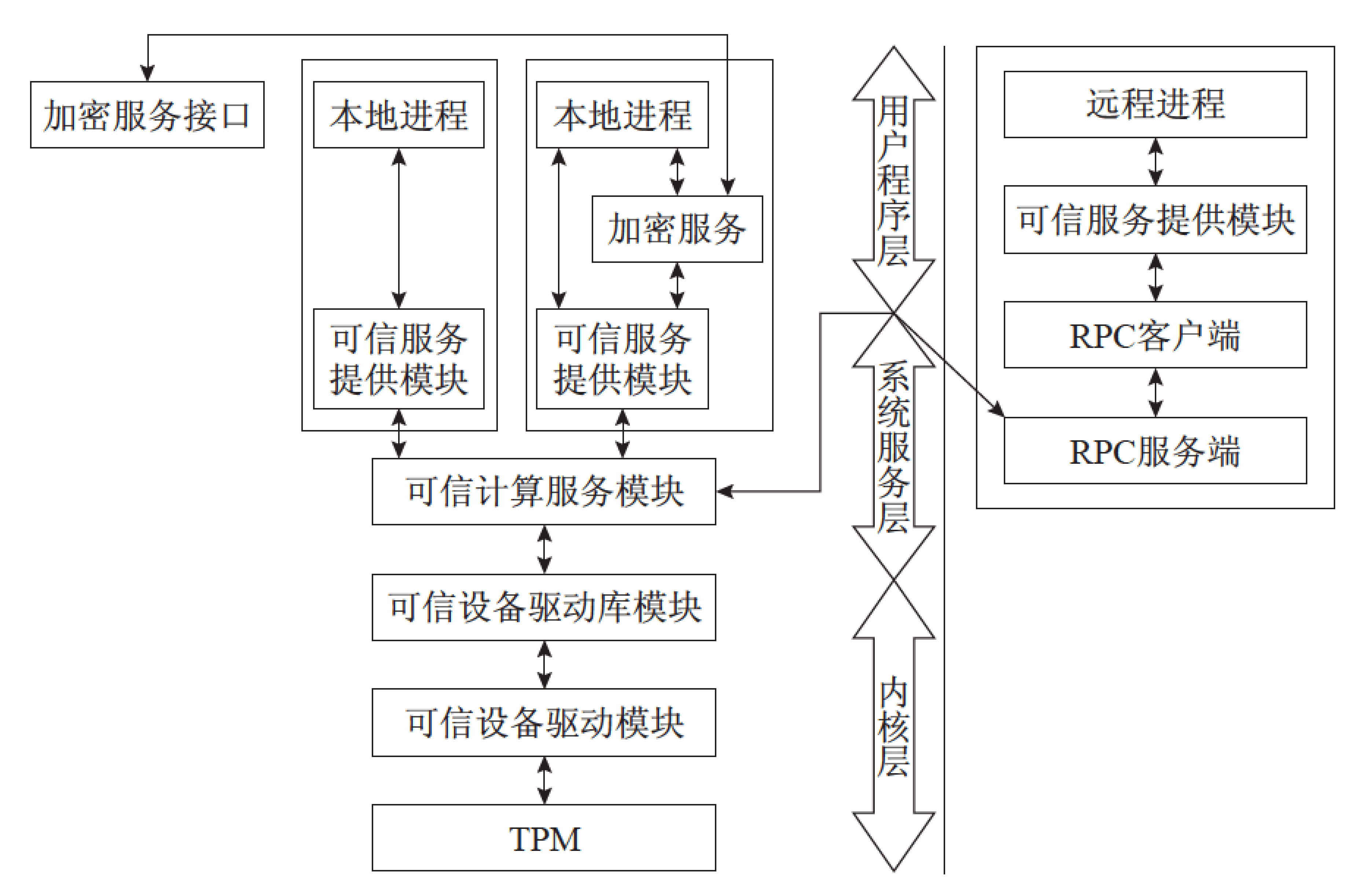


图8-13　可信计算软件栈结构框图

5）可信网络连接技术

可信网络连接包括可信协议，可信构件及可信连接接口。

① 可信协议：可信协议部署在当前网络协议的不同层次，用来实现网络环境中终端平台间的相互通信。

② 可信构件：可信构件包括防病毒构件、防火墙构件、系统补丁管理构件和系统完整性测量构件，其分布在终端系统和服务器中，负责完成手机系统硬件和软件的配置信息，并通过终端可信代理软件将这些信息提供给服务器。

③ 可信连接接口：包括终端安全代理软件之间、终端主机、网络设备及策略服务器之间的接口等，用于完成可信信息的交换。

可信网络连接的框架如图8-14所示，客户端访问请求端点向服务器端发出访问请求，服务器端根据设定的访问策略决定是否允许客户端接入网络，并且由策略执行端的网络设备执行允许客户端接入网络或拒绝客户端接入网络的决定。

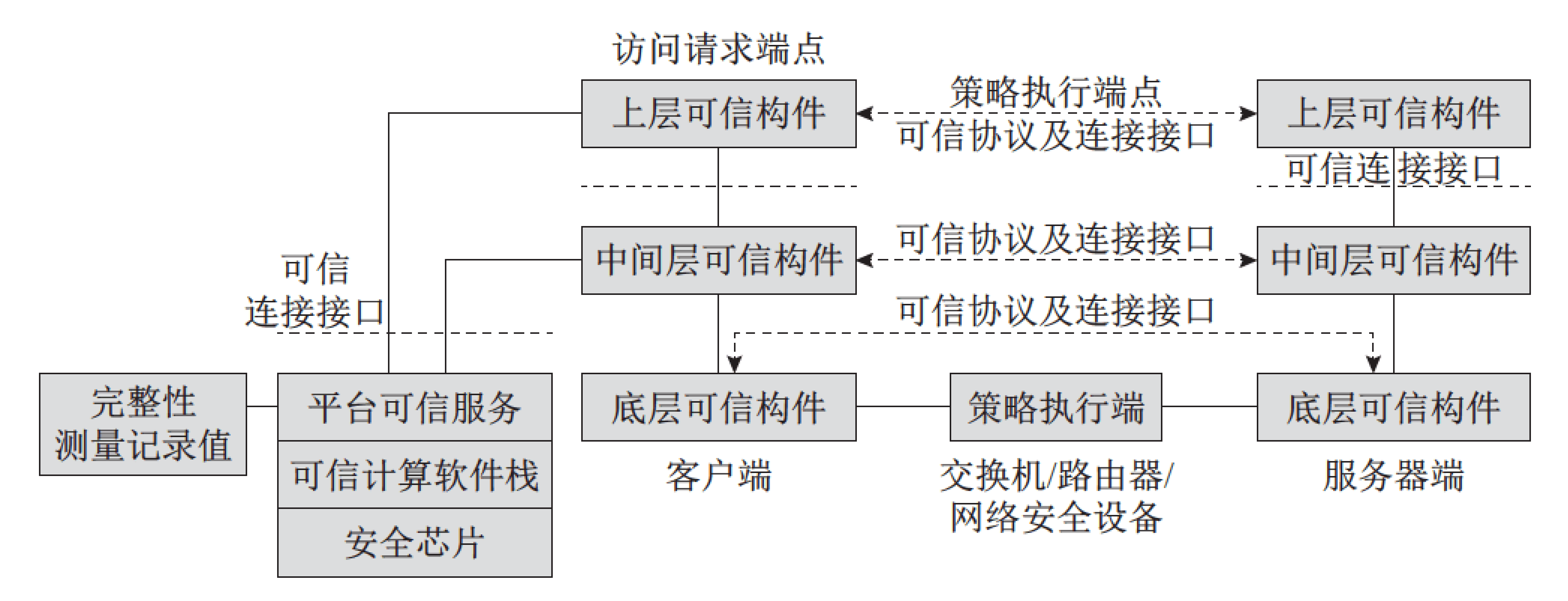


图8-14　可信网络连接框图

8.5.2 量子通信技术

1. 概述

量子通信技术利用量子不确定性原理与量子态不可克隆的特性来进行安全密钥分发，理论上可实现不可破译的安全加密通信，典型应用包括量子信息传送和量子保密通信。其中量子保密通信能够解决传统通信加密算法易被破解和传输过程易被监听两大难题，技术相对成熟，具备实用化条件。

配电网是指从电源侧（输电网和发电设施）接受电能，并通过配电设施就地或逐级分配给各类用户的电力网络，是电网与用户连接的重要纽带。为了提高配电网运营管理水平和供电可靠性水平，公司建设了配电自动化、用电信息采集等智能化业务系统及与之相适应的通信系统，并且部署了数量庞大、分布广泛的各类业务终端、通信终端。

量子保密通信技术可进行安全密钥分发，攻击者无法测量和复制密钥（量子态），且一旦进行窃听即会被发现，具有比传统密钥分发机制更高的安全性，也是目前实用化程度最高的量子技术。因此，利用量子保密通信技术进行配用电业务身份认证、数据加密等环节所需密钥的分发，并探索与现有安全防护措施之间的兼容机制，对于提升配用电业务信息安全防护能力具有重要意义。

2. 基本原理

目前，量子密钥分配和量子隐形态传输技术都被称为量子通信。其中，量子隐形态传输技术还停留在理论研究和实验阶段，已经初步实用化的量子通信技术是量子密钥分配。量子密钥分配其实依旧依托于光纤通信，而单光子具有不可分割性是量子密码安全性的物理基础，因而量子密钥分配并非颠覆经典通信，而是给经典通信增加了一把量子密码锁。

具体做法是用弱相干光源发射光子，因为弱相干光源弱到一定程度，光子是一个一个往外蹦的，以此代替单光子源。把一个信息编码在一个光子上，一个光子有着不同的量子态，代表着0和 1，把光子通过光纤发射过去，接收方接到密钥后进行解码。

量子密钥分配可以建立安全的通信密码，通过一次一密的加密方式可以实现点对点方式的安全经典通信。

光子具有不可分割性，在单光子发射的情况下，窃听者不可能将光子切成两半，拿走一半获得密钥，一半传输给接收方；光子不可能被准确复制，所以窃听者无法通过复制光子获取信息；光子无法准确测量，所以窃听者无法通过准确测量光子，制备出一个一模一样的光子。总而言之，窃听者无法将一个光子变成一模一样的两个光子，或者无法将光子信息读取出来后将光子再发出去。一个未知的量子态是唯一的，接收者如果接收到了准确的光子，那么窃听者就拿不到任何信息。

但弱相干光源发射出去的是单光子与多光子脉冲的概率混合，在所发出的非真空脉冲

中，有些是单光子的，有些是多光子的，例如2光子、3光子……多光子脉冲即包含了多个全同偏振光子。而多光子脉冲不再拥有不可分割性，在这种情况下，窃听者可将其分离，自己留下一个，将剩余光子送到远程合法用户，且窃听者的行为不会被合法用户察觉。

为了应对光子数分离攻击，可以用诱骗信号量子密码方案应对。用弱光替代单光子，有可能存在多个光子的概率，也有可能存在1个光子的概率。诱骗态方法是指发射2或3种不同强度的全同偏振光子，经过信道衰减后，强度高的光子到达的概率高，强度低的光子达到的概率低，在正常状态下，这个概率是成正比的。如果窃听者采取从多个全同偏振光子中拿走一个的方法获取信息，那么光子的接收概率会和正常状态下不一样，这样就可以监测出是否被窃听。

量子保密通信技术能够为配用电业务传输提供更强的安全防护能力，确保配电网安全稳定运行以及用户用电信息安全。基于量子保密通信技术能够提升信息传输过程中被非法获取、篡改的难度，避免“遥控”指令被破译导致的安全风险，及终端被“劫持”“旁路”进而反向入侵主站导致的系统失控风险，从而提升配电网安全稳定运行水平。基于量子保密通信技术可有效防止用户信息被篡改或隐私泄漏的可能性，保障用户用电信息、计费信息的准确无误传输，提升电网服务质量。

3. 关键技术

虽然加密数据传输载体可以继续使用国网已有的光纤网络，且单光纤的数据传输性能不会受到影响，但需要单独为量子传输分配独立的光纤通道，部分机房光纤出口资源已非常紧张，新建光纤通道建设成本较大，可租用的已有量子通信网络仅有“京沪干线”；尚未制定针对电力行业量子通信设备接口的协议标准，在已有电力通信设备上增加量子保密通信设备存在一定的困难；针对电力应用，需要研制专用量子保密通信设备，尤其是针对变电站、特高压输电线路等强电磁应用环境，量子保密通信设备需要满足防护等级。

① 研究配用电业务的量子保密通信体系架构。量子密钥协商生成目前只能依靠独立纤芯光纤完成，而承载配用电业务的网络除了光网络以外，还包括以太网、无线公网、无线专网等，通信双方不具备在线协商生成量子密钥的通道。同时，业务终端数量庞大、型式各异、安装环境复杂，业务主站与终端之间直接协商生成量子密钥存在较大的实现难度。

② 研究量子保密通信技术与已有认证及保密通信技术之间的兼容机制。将量子保密通信技术应用于配用电场景时，应当充分考虑当前已经存在的认证及保密通信技术体制，研究并提出相适应的认证及通信兼容方案，使业务系统具备在两种保密技术之间进行切换的能力，满足配用电安全防护、业务传输时延、系统处理效率等方面的要求是关键点。

③ 研究量子通信系统信道受光缆信道条件影响情况。量子通信系统的密钥生成率和平均误码率等关键指标受光缆信道的影响非常大，弯曲损耗、偏振变化等物理损伤会直接降低系统的通信质量。量子通信设备和架空电力光缆直接同空气接触，温度湿度变化、风力大小方向、降雨等因素将直接迅速地被量子通信设备和光缆介质感知，进而改变损耗、

色散、偏振等系统状态，从而引起光缆以及量子通信设备性能参数的变化，最终影响量子通信系统的质量。

④ 研究多业务智能识别及分级加密技术。除研究并实现量子密钥加解密功能之外，研究安全加密设备多业务快速智能识别技术实现业务分区传输，并在此基础上结合安全防护需求实现业务分级加密是需要研究的关键技术。

⑤ 研究终端侧量子密钥存储及管理方法。终端侧量子密钥借助量子密钥移动存储设备进行离线分发，研究量子密钥在各个分发环节中的安全存储及有效管理方法，实现量子密钥从汇聚侧到终端侧的安全、合法、正确分发及使用，是需要研究的关键点和难点。

⑥ 适用于电力架空光缆环境的偏振预调节方法。量子通信一般利用光子的偏振特性或相位特性进行编码，对于两种编码方式，长距离光纤传输引起的光的偏振性退化会造成误码率的增加。同时，在架空光缆的环境下，光子偏振态在光纤中传输时受垂摆和舞动等影响非常大，将发生剧烈的无规则变化，这将进一步给系统引入较大的误码率，甚至导致量子密钥生成设备不能正常运行成码。因此，为保证量子通信的稳定和畅通，有必要研究架空光纤中偏振态的测量、控制和损伤补偿技术，快速偏振反馈正是实现这一需求的关键点及难点。

需围绕反馈型偏振稳定和补偿架构，测试各种监测方法的有效性，将粒子群优化算法（Particle Swarm Optimization，PSO）引入偏振模色散自适应补偿，作为搜索算法和跟踪算法，克服以往算法难以适应多自由度补偿、不具备抗噪性、易陷入局部极值等缺点。

8.5.3 光锁技术

1. 概述

光通信抵近噪声微元传输物理层安全技术，是目前国内唯一能够实现集高速率传输和高强度安全于一体的光通信安全技术，填补了网络物理层光通信安全空白。

该技术建立了光通信的“微元-噪声”安全体系框架，利用物理随机噪声加密和隐藏微元信号，基于抵近噪声微元传输信道对信噪比敏感的特点进行光纤窃听入侵检测，取得了超阶调制、多维域加密等系列安全技术创新，首次在同一光通信技术体制下实现了加密、隐藏和窃听发现的一体化功能。

该技术提出的光通信抵近噪声微元传输物理层安全方案，在几乎不牺牲系统传输性能的前提下实现了高速率通信保密一体化安全，从根本上解决了光通信传输效率与安全强度之间的突出矛盾，与现有光通信系统和线路设施具有良好的兼容性。同时，该技术为实现逼近信息论安全提供了一条可行的技术创新途径，对增强我国网络空间信息安全防御能力具有重大战略意义。

2. 基本原理

在传统光纤通信中，光噪声会造成信号接收质量下降，需要尽可能消除噪声带来的影响。但是，微元噪声加密技术巧妙利用光噪声作为随机源/干扰源，加密/隐藏信号的真实状态，与传统光纤通信的主要区别是：传统通信基于远离噪声光通信机制设计，即传统通信光噪声造成接收质量下降，需要尽可能消除其影响；而抵近噪声光通信技术则巧妙利用光噪声作为随机源/干扰源，加密/隐藏信号物理状态。其中光噪声和微元的重要概念和关键特性包括：

1）光噪声

光噪声（photon noise）来源：激光器固有量子噪声、光放大器固有的ASE噪声特性。

噪声具备如下几项特征：天然性（天然存在，无法避免）；随机性（随机涨落，无法复制）；物理性（物理现象，多维呈现）；模拟性（模拟过程，复杂连续）。

2）微元

微元：信号表达的物理状态，指传输时由于噪声影响能够分辨的最精细信号状态，利用“阶”和“维”来进行度物理量。

线微元：选择某一物理“维”度将微元细分为众多“阶”状态，直到相邻“阶”光噪声被淹没而无法区别（称为“超阶调制”）。

点微元：在各个物理“维”度上构造线微元，并统一表达形成点微元，点微元对应不同维度的“阶”状态均被光噪声淹没而无法精确测量。

3. 关键技术

1）抵近噪声超阶调制与微元光电变换关键技术

现有基于光信号处理和/或电信号处理的物理层安全技术中，已经提出的解决方案主要有光量子通信体制、光跳频通信体制、光混沌通信体制、光码分复用体制、光隐蔽通信体制、光多入多出通信体制等。实现物理层传输安全的主要手段包括光加密、光隐藏和窃听发现三类功能。上述解决方案，在同一技术体制下支持实现一种或两种安全功能，例如光量子通信体制支持窃听发现功能、光跳频通信支持加密功能、光混沌通信/码分复用/隐蔽通信支持加密和隐藏功能等。

抵近噪声微元传输光通信方案，可以在相同的光通信技术体制下，采用各种方式的光信号处理和/或电信号处理手段，实现集加密、隐藏和窃听发现功能于一体的光通信物理层安全方案与产品，为满足传输高速率、安全高强度的要求提供了可靠保障。

在处理过程中，0、1信息是一个数字化的概念，而光信号本身在线路传输时总是以一定的物理形态呈现。光锁系统认为这些物理状态由很多个微元分量所体现，并携带比特信息。作为载体的微元分量之间相互作用、相互交联，最后在物理上构成实际传输的信号流。所以，光锁系统线路传输的是由微元分量构成的信号，这些微元被处理、再组合，最

后以类似模拟信号的传输方式呈现在线路上。

微元的处理与组合受到密钥约束，从而实现了传输过程本身对信号的加密功能。在微元理论模型下，原始二元信息、映射关系与密钥三者共同交织形成以微元表达的物理状态，使得密钥的穷举空间暴涨，从密钥控制的微元状态回溯原始二元信息的路径复杂难寻，从而极大增加了破解难度。

微元化后的信号加密空间可扩展至时间、频率、幅度、相位、偏振等维度，规则加密的效果更加显著。利用微元（代表确定性）和光噪声（代表非确定性）作用关系，可建立集加密、隐藏和窃听发现于一体的光纤通信“微元-噪声”安全体系框架安全。

2）抵近噪声微元传输逼近信息论安全关键技术

目前在各种光通信安全技术体制中，除了量子通信已被严格证明理论上满足信息论安全（也称为无条件安全或绝对安全）之外，其他技术手段由于不具备窃听发现能力，都无法做到系统无条件安全。光锁技术提出的抵近噪声微元传输光通信方案，利用抵近噪声微元传输通道对信噪比敏感的特点，实时监控光纤线路中信号与噪声状态的变化，分析检测入侵行为，实现窃听发现功能，对已被窃听的信号实施丢弃策略，从而保证了光通信系统的整体安全性能逼近信息论安全。

除了利用上述微元构造方式，还可以结合光纤通信物理层的时、空、频、幅、相、偏等各个维度构造全维度点微元。利用全维度点微元对噪声敏感的特性测量接收信噪比变化发现窃听行为，做到“你来拿、我不用”，窃听方即使拥有无限计算能力也无法截取信息，达到逼近信息论安全。

8.5.4 区块链技术

1. 概述

区块链是比特币的基础支撑技术，区块链技术的突出优势在于去中心化设计，通过运用加密算法、时间戳、树形结构、共识机制和奖励机制，在节点无须信任的分布式网络中实现基于去中心化信用的点到点交易，解决了目前中心化模式存在的可靠性差、安全性低、高成本、低效率等问题。

区块链技术被认为是继大型计算机、个人计算机、互联网、移动社交之后的第五次颠覆式计算范式。区块链是一种按照时间顺序将数据区块用类似链表的方式组成的数据结构，并以密码学方式保证不可篡改和不可伪造的分布式去中心化账本，能够安全存储简单的、有先后关系的、能在系统内进行验证的数据。区块链使用“工作量证明”（Proof of Work，PoW）及“权益证明”（Proof of Stake，PoS）或其他共识机制，再加上加密技术，使一个不可信网络变成可信网络，所有参与者可以在某些方面达成一致，而无须信任单个节点。

区块链具有去中心化、网络健壮、灵活、安全可信等特点。首先，区块链采用纯数

学的方法建立分布式节点间的信任关系，形成去中心化的可信分布式系统，产生交易、验证交易、记录交易信息、进行同步等活动均是基于分布式网络完成的，是彻彻底底的去中心化。其次，区块链采用独特的经济激励机制来吸引节点完成工作（如挖矿），促使节点提供算力或其他资源，保证整个分布式网络的顺利运行。整个分布式网络所容纳的节点越多，其健壮性越强，除非一半以上的节点同时出现问题，否则分布式网络将会一直安全运行。再次，区块链提供用户可编程的脚本系统，大大增加了区块链应用的灵活性。在以太坊（Ethereum）中，更加完备、功能更加强大的脚本系统智能合约，使更为复杂、更为高级的分布式应用得以实现。最后，区块链的安全性是加密技术所保证的，整个分布式网络所提供的算力是非常惊人的，想要篡改区块链中的数据，只是在理论上可行，但是所花费的电力、设备等成本将得不偿失。

2. 基本原理

比特币和以太坊是两种具代表性的区块链技术应用，一个是区块链技术的起源，另一个是区块链2.0的代表应用。

比特币和以太坊的基础架构如图8-15所示。图8-15中虚线表示的是以太坊与比特币的不同之处。总体来说，数字货币的区块链系统包含底层的交易数据、狭义的分布式账本、重要的共识机制、完整可靠的分布式网络、网络之上的分布式应用这几个要素。底层的数据被组织成区块这一数据结构，各个区块按照时间顺序链接成区块链，全分布式网络的各个节点分别保存一份名为区块链的分布式账本，网络中使用 P2P 协议进行通信，通过共识机制达成一致，基于这些基础产生相对高级的各种应用。在该架构中，不可篡改的区块链数据结构、分布式网络的共识机制、工作量证明机制和愈发灵活的智能合约是具代表性的创新点。

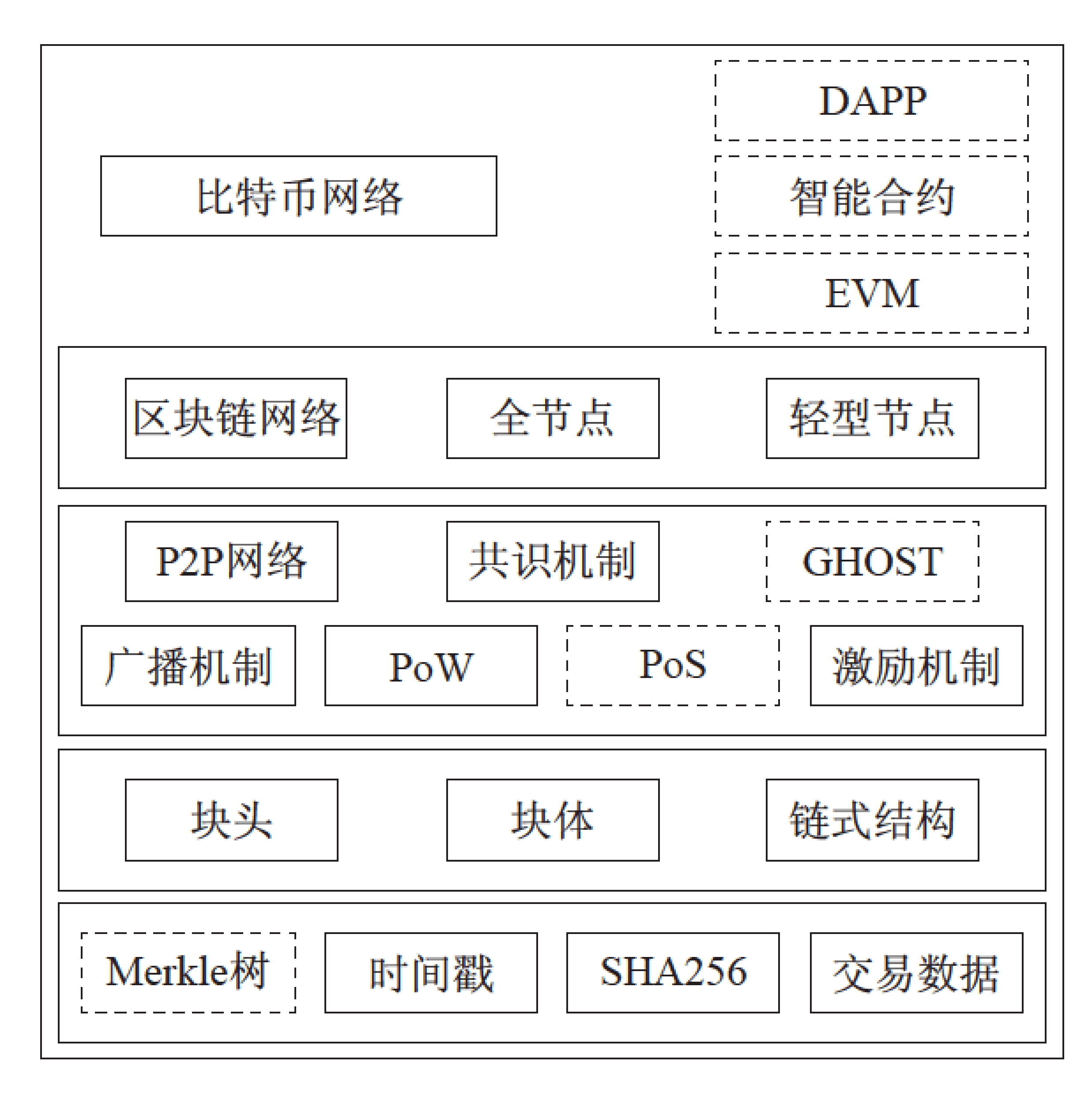


图8-15　区块链基础架构

3. 关键技术

1）底层数据

在区块链系统中，底层数据并不是存储在区块链中的数据，这些原始数据需要进一步加工才能被写入区块内。底层数据最根本的是交易记录，其他数据只是为了对消息记录进行封装。

交易数据：交易数据是带有一定格式的交易信息，以比特币为例，一条比特币交易信息应包含以下字段：4B的版本信息，用来明确这笔交易参照的规则；1～9B的输入计数器，表示被包含的输入数量；变长字节的输入，表示一个或多个交易输入（地址）；1～9B的输出计数器，表示被包含的输出数量；变长字节的输出，表示一个或多个输出（地址）；4B的时钟时间，表示一个UNIX时间戳或区块号。

时间戳：时间戳被用来加盖在区块头中，确定了区块的写入时间，同时也使区块链具有时序的性质，时间戳可以作为区块数据的存在性证明，有助于形成不可篡改不可伪造的分布式账本。更为重要的是，时间戳为未来给予区块链技术的互联网和大数据增加了时间维度，使通过区块数据和时间戳来重现历史成为可能。

SHA256算法：区块链不会直接保存明文的原始交易记录，只是将原始交易记录经过散列运算，得到一定长度的散列值，将这串字母与数字组成的定长字符串记录进区块。比特币使用双SHA256散列函数，将任意长度的原始交易记录经过2次SHA256散列运算，得到一串256b的散列值，便于存储和查找。散列函数具有单向性、定时性、定长性和随机性的优点。单向性指由散列值无法反推得到原来的输入数据（理论上可以，实际几乎不可能），定时性指不同长度的数据计算散列值所需要的时间基本一样，定长性指输出的散列值都是相同长度，随机性指2个相似的输入却有截然不同的输出。同时，SHA256函数也是比特币所使用的算力证明，矿工们寻找一个随机数，使新区块头的双 SHA256 散列值小于或等于一个目标散列值，并且加入难度值，使这个数学问题的解决时间平均为10min，也就是平均每10 min产生一个新的区块。

Merkle 树：Merkle树是区块链技术的重要组成部分，将已经运算为散列值的交易信息按照二叉树形结构组织起来，保存在区块的块体之中。Merkle 树的生成过程是：将区块数据分组进行散列函数运算，将新的散列值放回，再重新拿出2个数据进行运算，一直递归下去，直到剩下唯一的“Merkle 根”。比特币采用经典的二叉Merkle树，而以太坊采用了改进的Merkle Patricia树。Merkle树的优点有：良好的扩展性，不管交易数据怎么样，都可以生成一棵Merkle树；查找算法的时间复杂度很低，从底层溯源查找到Merkle根部来验证一笔交易是否存在或合法，时间复杂度为lbN，极大降低运行时的资源占用；使轻节点成为可能，轻节点不用保存全部的区块链数据，仅需要保存包含Merkle根的块头，就可以验证交易的合法性。

2）分布式记账本

使用分布式记账本来代替区块链，是为了区别狭义的区块链和广义的区块链技术，前者是分布式记账本这一时序链式数据结构，后者是个完整的带有数学证明的系统框架。狭义的区块链结构如图8-16所示，每个区块分为块头和块体两部分，所有区块按照时序相链接，形成狭义上的区块链。

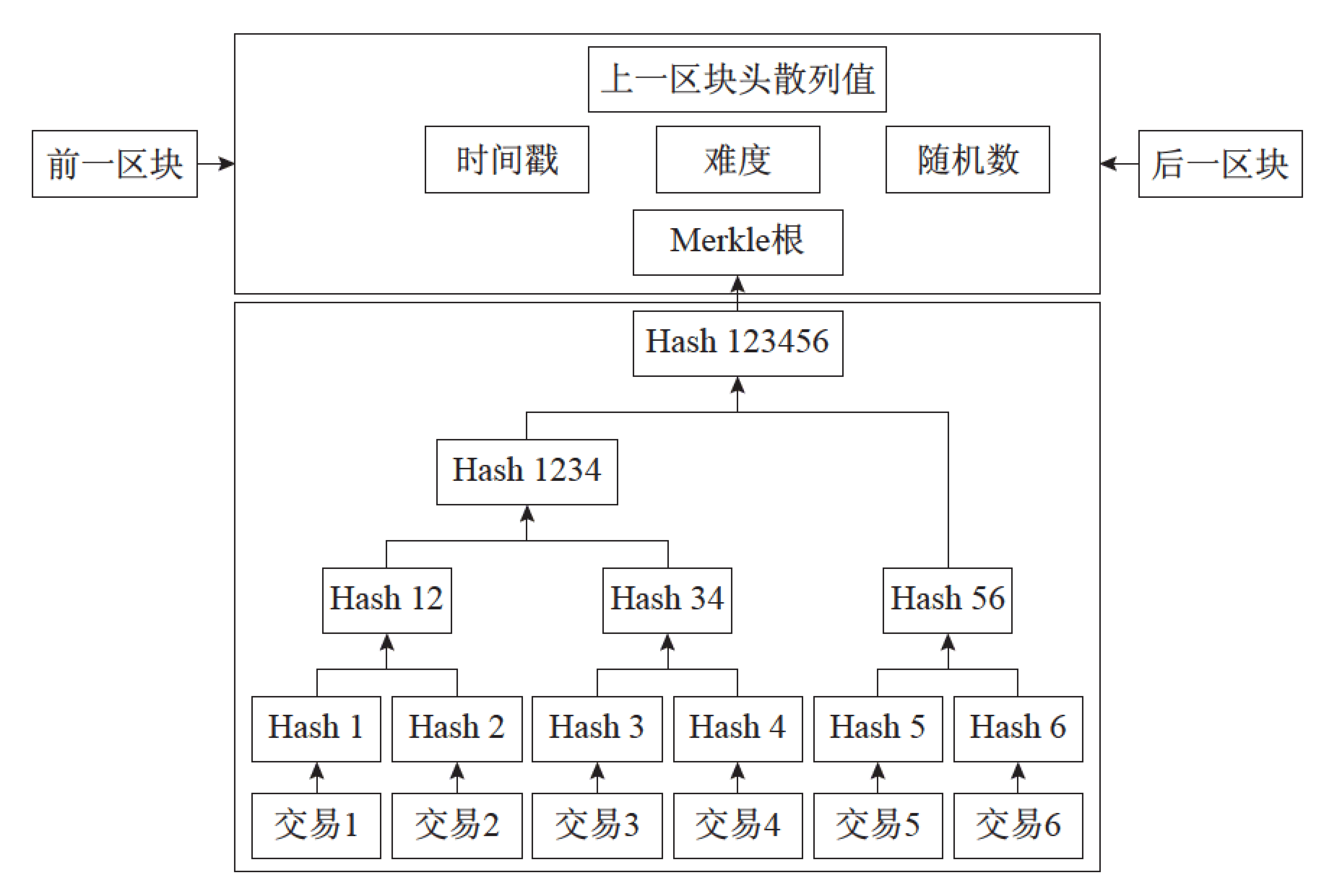


图8-16　分布式记账本模型

区块头：区块头的内容有上一区块头的散列值、时间戳、当前PoW计算难度值、当前区块PoW问题的解（满足要求的随机数），以及Merkle根。以比特币为例，具体的数据格式为：4B的版本字段，用来描述软件版本号；32B（256b）的父区块头散列值；32（256b）字节的 Merkle根；4B的时间戳；4B的难度目标；4B的Nonce（随机数，问题的解）。区块头设计是整个区块链设计中极为重要的一环，区块头包含了整个区块的信息，可以唯一地标识出一个区块在链中的位置，还可以参与交易合法性的验证，同时体积小（一般不到整个区块的千分之一），为轻量级客户端的实现提供依据。

区块体：区块体包含了一个区块的完整交易信息，以Merkle树的形式组织在一起。如图8-16所示，Merkle树的构建过程是一个递归计算散列值的过程，交易1经过 SHA256计算得到Hash 1，交易2同样算得Hash 2，将2个散列值串联起来，再做 SHA256计算，得到Hash12，这样一层一层地递归计算散列值，直到最后剩下一个根，就是Merkle根。可以看到，Merkle树的可扩展性很好，不管交易记录有多少，最后都可以产生Merkle树以及定长的Merkle根。同时，Merkle树的结构保证了查找的高效性，N个叶子节点的Merkle树最长查找路径长度为lbN，这种高效在大交易规模中异常明显。

链式结构：除了创世区块以外，所有区块均通过包含上一区块头的散列值的方法构成

一条区块链。同时，由于包含了时间戳，区块链还带有时序性。时间越久的区块后面所链接的区块越多，修改该区块所花费的代价也就越高，区块链在增加新区块的时候，有很小的概率发生“分叉”现象，即同一时间挖出2个符合要求的区块。对于“分叉”的解决方法是延长时间，等待下一个区块生成，选择长度最长的支链添加到主链。“分叉”发生的概率很小，多次分叉的概率基本可以忽略不计，“分叉”只是短暂的状态，最终的区块链必然是唯一确定的最长链。

创世区块：每一个区块链都有一个特殊的头区块，不管从哪个区块开始追溯，最终都会到达这个头区块，即创世区块。

3）组网方式和核心机制

狭义的区块链，即分布式账本，将这个账本用起来才是区块链技术的关键所在。基于分布式账本之上的区块链网络，采用对等式网络——P2P网络（Peer-to-Peer network）将所有节点连接在一起，设计PoW或其他共识机制使无信任基础的双方在不需要第三方的情况下建立互信，使用广播的方式传播交易信息，加上激励机制来保证节点提供算力以维持整个网络的顺利运行。

P2P网络：区块链网络的去中心化来自于采用P2P组网方式，网络中每个节点均地位对等且以扁平式拓扑结构相互连通和交互，不存在任何中心化的特殊节点和层级结构，每个节点均会承担网络路由、验证交易信息、传播交易信息、发现新节点等工作。

广播机制：区块链网络公布交易信息的方式是广播，生成交易信息的节点先将信息广播到相连接的节点，节点验证通过后就会再进行广播，信息会以极快的方式被全网中的节点接收。实际上，并不需要全部节点都保留这条交易信息，只要保证大多数（51%）节点接收到，就可以认为交易通过。如果这条交易信息有问题，如交易者的余额不足以支付，接收到错误消息的节点验证不通过，就会废弃该交易数据，不会对它再进行广播。新区块的生成也是通过广播来确认的，找到满足条件的随机数后进行广播，经过验证后确认新区块的记账权，生成新的区块，全网进行同步，将该块添加到主链上。

共识机制：分布式网络的核心难题是如何高效地达成共识，就像现有的社会系统，中心化程度高的、决策权集中的社会更容易达成共识，像独裁和专制，但是社会的满意度很低；中心化程度低的、决策权分散的社会更难达成一致，像民主投票，但是整个社会的满意度更高。“任何基于网络的数据共享系统，都最多拥有以下3条中的2条：数据一致性（C）；对数据更新具备高可用性（A）；能容忍的网络分区（P）”，即 CAP 理论。分布式网络已经带有了P，那么C或A只能在两者中选择一条。如何在一致性和可用性之间进行平衡，在不影响实际使用体验的前提下还能保证相对可靠的一致性，是研究共识机制的目标。早期的比特币采用高度依赖节点算力的PoW机制来保证比特币网络分布式记账的一致性，随着各种竞争币种的发行，更多相似的共识机制得以出现，PoS 是一种基于PoW并且进行了改进的共识机制。

PoW共识机制：PoW机制是由中本聪所设计的适用于比特币系统的共识机制，其核心

思想是通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性。在比特币中，所有参与“挖矿”的节点都在遍历寻找一个随机数，这个随机数使当前区块的区块头的双SHA256运算结果小于或等于某个值。找到符合要求的随机数的节点即获得当前区块的记账权，获得一定数额的比特币作为奖励。另外，引入动态难度值，使求解该数学问题所花费的时间在 10min左右。PoW共识机制具有十分重要的意义，将比特币的发行、交易和记录完美地联系起来，同时还保证了记账权的随机性，确保比特币系统的安全和去中心化。

GHOST（Greedy Heaviest Observed Subtree）协议：该协议是为了解决比特币使用 PoW 算力竞争引起的高废块率带来的算力浪费问题。废区块指的是在新块广播确认的时间里“挖”出的符合要求的区块。GHOST 协议提出在计算最长链时把废区块也包含起来，即在比较哪一个区块具有更多的工作量证明时，不仅有父区块及其祖先区块，还添加其祖先区块的作废后代区块来计算哪个块拥有最大的工作量证明。在以太坊中，采用了简化版GHOST协议，废区块只在五代之间参与工作量证明，并且废区块的发现者也会收到一定数量的以太币作为奖励。

PoS共识机制：PoW共识机制有明显的缺点，算力资源被过多地浪费掉，PoS共识机制是为了解决PoW的缺陷而提出的替代方案。PoS本质上是采用权益证明来代替PoW的算力证明，记账权由最高权益的节点获得，而不是最高算力的节点。权益证明就是资源证明，拥有最多资源的节点挖矿的难度最小。以太坊目前采用的仍然是PoW，但是正在开发的下一版本将会转为PoS共识机制。

激励机制：激励机制是区块链技术中的重要一环，以比特币为例，开采出新的区块的节点会得到一定数量的比特币和记账权，记账权使节点在处理交易数据的时候得到交易费用。比特币的交易费用基于自愿原则，提供交易费用的交易会被优先处理，而不含交易费用的交易会先放在交易池中，随时间的增加而增加其优先级，最终还是会被处理。激励机制保证了整个区块链网络的持续向外扩张，促使全节点提供资源，自发维护整个网络。以比特币为例，目前整个比特币网络的算力已经达到 800 000 000Gh/s，超过了全球Top 500超级计算机的算力总和，想要对整个比特币网络做出影响几乎不可能。

4）区块链节点

在最初的区块链网络设计中，不存在任何中心化的特殊节点和层级结构，每个节点完全对等，承担着网络路由、验证交易信息、传播交易信息、发现新节点等工作。但是实际上物理设备是存在明显性能差距的，以比特币网络为例，可作为节点的设备有个人计算机、服务器、专为比特币挖矿设计的矿机，以及移动端，它们提供的算力相差了几个数量级，并且存储空间也不同。

想要将移动端作为全节点无疑是不现实的。于是有了全节点和轻型节点，全节点是传统意义上的区块链节点，包含有完整的区块链数据，支持全部区块链节点的功能。全节点通常是高性能的计算设备，比特币刚面世时依靠CPU来提供算力，后来使用GPU，发展到现在是专门设计将SHA256 算法固化到硬件的矿机，算力成几何增长趋势。轻型节点是依

靠全节点存在的节点，不用为区块链网络提供算力，只保存区块链的区块头，由于区块头包含了Merkle根，可以对交易进行验证。轻型节点多为移动端，如智能手机、平板电脑、移动计算机等。

5）智能合约

区块链技术的智能合约是一组情景——应对型的程序化规则和逻辑，是部署在区块链上的去中心化、可信息共享的程序代码。签署合约的各方就合约内容达成一致，以智能合约的形式部署在区块链上，即可不依赖任何中心机构自动化地代表各签署方执行合约。智能合约具有自治、去中心化等特点，一旦启动就会自动运行，不需要任何合约签署方的干预。

智能合约的运行过程如下：智能合约封装预定义的若干状态、转换规则、触发条件以及对应操作等，经过各方签署后，以程序代码的形式附着在区块链数据上，经过区块链网络的传播和验证后被记入各个节点的分布式账本中，区块链可以实时监控整个智能合约的状态，在确认满足特定的触发条件后激活并执行合约。智能合约对区块链有重要的意义，智能合约不仅赋予了区块链底层数据可编程性，为区块链2.0 和区块链 3.0奠定了基础，还封装了区块链网络中各节点的复杂行为，为建立基于区块链技术的上层应用提供方便的接口。拥有了智能合约的区块链技术前景极为广阔，甚至可与物联网相结合，在智能家居领域实现智能自动化，如室内温度湿度亮度的自动控制、自动门允许特定的人进入等。

现有水平的智能合约及其应用本质逻辑上还是根据预定义场景的IF-THEN类型的条件响应规则，能够满足目前自动化交易和数据处理的需求。未来的智能合约应具备根据未知场景的WHAT-IF推演、计算实验和一定程度上的自主决策功能，从而实现由目前的“自动化”合约向真正的“智能”合约的飞跃。

8.6 新技术应用与路线预测

8.6.1 总体趋势

未来十年以及更长时间，随着能源互联网向国际化发展、智能电网更加坚强，主动配电网支撑更多业务，作为重要支撑的接入网必将引入国际标准，国际化将成为接入网重要特征之一。随着分布式能源、储能以及核能等清洁电源接入电网，随时上网就地用电需要电力通信提供更快、更宽的通信信道支撑多监测、多控制、双向通信业务，广覆盖、低延时、高可靠、智能化将成为接入网重要特征。随着电力体制改革的推进以及电力市场的建立，充分利用接入网资源催生新技术、新产品、新模式、新业态，以开放的态度融合多种通信技术支撑电网发展，全方位促进创新。在管理、技术、安全三方面的提升保障了电力

通信安全可靠的运行，助推国民经济及社会发展。

8.6.2 新技术的电力应用

1. 无线专网技术

未来无线专网可广泛应用于从发电、输电、配电到用电、调度、信息化等的整个智能电网业务环节中，如配网自动化、计量自动化（远程抄表）、视频传输（配电房监控）、移动巡检、移动办公（作业表单）、门禁监控、电动汽车充电桩远程操作、作为IMS 系统的无线接入部分实现IMS的移动化应用等。另外在新变电站建设时，无线专网可作为现场建设调度指挥系统并为自动化等设备调试提供临时通信通道。

总之，电力无线专网不仅可作为现阶段配电自动化、计量自动化、移动办公等电力业务的有效通信方式，还可以满足未来智能电网通信网向电力物联网发展的大数据通信需求。

1）可见光技术电力应用

目前可见光通信的研究分化为三个方向：一是低速窄带方向；二是中高速宽带方向；三是超高速方向。低速窄带方向包括隧道、井下、超市等特殊场景的定位与通信，目前已有部分示范应用；中高速宽带方向包括超高速无线光互联通信、室外拓展距离可见光通信、水下可见光通信等，目前尚处于演示系统阶段；超高速方向尚处于科研与实验验证阶段。

2）NB-IOT技术电力应用

目前，电网进入能源互联时代，需要广泛海量的数据连接支持，如电器设备温度、用户电器运行状态、配电故障指示状态，智能表计量数据等。这些数据与已经连接的诸如“三遥”数据相比，是“小数据”，具有显著的自身特性：业务相关性强、系统运维中对此类数据需求强烈；海量数据，分布广、分散性强，部分不易供电，连接难；单数据价值密度低，集合后呈大数据特征，蕴含价值高；状态变化缓慢稳定，呈现稳态特性，采集频次需求低；日常关注度低，影响较大。而NB-IoT特别适用于此类小数据连接的场景，与现有电力通信专网融合，将成为能源互联网发展的重要支撑。

在能源互联网“泛感知”的需求下，运营级能源电力物联专网方案可通过一张网、共平台、多业务应用场景的图景，为智慧能源提供低成本的物联解决方案，物联网将以终端通信接入网为支撑进行拓展，深化智慧能源互联网的发展应用。

3）LoRa技术电力应用

LoRa技术在电网中可用于外线电缆防盗检测，电力输电、配电网故障指示器远程检测、远程电表抄表等场景中。

LoRa技术可用于电力监控领域。电力故障指示器是在电力输电和配电中使用较多的设备，但通常依赖电力光缆或特殊通信信道传输。对于无人区，目前的多种通信方式都达不到要求，但通过配置，可使用LoRa技术对电力输电、配电网故障指示器远程检测。

LoRa可用于智能抄表领域。在电力系统的运营过程中，传统的人工抄表方式有人力耗费大、误差大等缺点，有些电表安装地点偏远，有些则需要带电作业，除了造成资源浪费和安全隐患外，在实时性、准确性和应用性等方面都存在诸多不足之处。使用LoRa模块实现的远程抄表系统不仅拥有覆盖广、通信成本低等特点，还能提高电力单位对抄表业务的管理规范性，解决布点分散的难题。

4）5G 技术电力应用预测

5G无线通信技术的发展方向主要体现在密集网络，终端直接通信，新型网络架构，高频段通信、网络智能化等方面。预计到2020年，各种物联网应用将得到广泛普及，如智能电网、智慧城市、移动医疗、车载娱乐、运动健身等。未来5G网络将支持虚拟现实、超清视频以及移动游戏等应用服务，这类移动交互式应用对无线接入带宽和通信时延有很高的需求。5G网络将在电力紧急语音通话、无人机远程监测、入侵监测、急救人员跟踪等场景得到应用，同时可为智能电网的信息化、自动化、互动化提供坚强支撑。

智能电网的通信系统覆盖了电力系统发电变电输电配电用电的全部环节，电力系统的发电设施形态规模以及能源管理与控制正在经历数字化变革的挑战，同时也在经历发电侧到用电侧向双向利用模式的转变，这些变革对构建大容量高速实时安全稳定的智能电网提出了如下需求：

通过5G与智能电网的结合，风力、太阳能等新能源并网业务带来的随机性、间歇性和调峰能力不均衡，对配套的通信系统性能提出了挑战。

实时监测、输电/配电自动化管理，要求通信网络延时5～50ms，5G可满足。

除低时延外，5G有助于降低智能抄表等大连接业务的能源消耗，同时使电网更加可靠。

针对5G网络技术架构特点，进行网关控制转发分离、控制功能重构、信息连接管理和移动性管理、移动边缘内容及计算、按需组网、统一的多无线接入技术融合、无线Mesh和动态自组织网络、无线资源调度与共享、用户和业务的感知与处理、网络能力开发等关键技术等在电力无线中的应用。

2. 有线专网技术

EPON和GPON都有一个共同的技术起源：窄带PON→A/BPON。GPON汲取ATM QoS、SDH OAM 以及 Ethernet开放架构的多种“源”头优势，形成面向未来光接入全业务网络的PON技术体系；基于创新的技术理念，EPON 延续 Ethernet开放架构单一“源”特点，形成强调数据接入业务能力的PON技术。

考虑光通信技术的发展现状、产品成熟及业务应用情况，未来五年到十年大带宽、远距离传输技术仍然以光纤网络为主，工业以太网和EPON作为两种主流的接入网通信技术，各有特点，目前在试点阶段均有应用，后续将根据不同项目的实际情况，各有优势，长期并存。

EPON和工业以太网在标准化、实时性、可靠性、安全性、带宽、技术成熟度及产业

链等方面具有优势，但由于光纤铺设成本高，组网成本偏高，运维成本高，适用于可铺设光缆且对安全、可靠性有严格要求的业务。

10G EPON系统的OLT和ONU均采用FPGA芯片，还处于功能研发和试商用阶段；目前已可支持QoS、VLAN、组播等典型功能，但不是稳定可靠的版本，在商用前还需大量调试和修改。据初步统计，全球现网部署的10G EPON规模已经超过25万线，其中大部分集中在中国。中国电信、中国联通、中国移动已进行多次10G EPON的性能测试，规模部署，不同厂家设备互通性已具备，可以在光纤到楼宇应用场景下商用，用户单位成本比EPON提高5%～20%，带宽提高了10倍。在需求和市场的推动下，PON技术的标准在持续演进中。10G EPON下一代演进路线是NG-EPON。

工业以太网技术具有稳定可靠、通信速率高、软硬件产品丰富、应用广泛以及支持技术成熟等优点，已成为最受欢迎的通信网络之一，相关设备厂商多，产业链较完整。工业以太网技术适用于节点较多、通信距离较长的业务场景，主要在数字化变电站中应用，上海、福建等单位在配电自动化配套通信网中也采用了工业以太网技术组网，应用效果良好。但工业以太网交换机通信协议的标准化程度不高，导致不同厂家的产品兼容性不够，影响网络运维效率。

10G EPON技术电力应用预测如下：

1）在中压配电网中的应用

我国中压配电网有多种接线方式，目前以星状和环状方式为主，通常可较方便地利用电力线路径资源建设通信光缆网络。鉴于中压配电网本身的自然属性，通信光缆网络一般宜采用星状或树状拓扑结构；在可靠性要求较高的地区，也可采用手拉手冗余保护结构。在组建中压配电网的通信网方面，PON技术的优势非常明显。PON由局侧OLT、用户侧ONU及其间的光配线网络（ODN）组成。ODN由光纤和无源设备（光分路器）组成。若承载可靠性要求较高的配电自动化业务，ONU可选择双PON接口，同时支持光路全保护方式，这样某一光纤中断时，业务可由另一光纤传输。接口可根据业务接入接口及上级通信网接口情况综合选择。

2）在用电信息采集中的应用

我国电表用户基数规模十分庞大。面对电力系统不断推广智能电表及其庞大电表数，电表信息远程自动采集技术将非常关键。这与互联网宽带业务末端接入的点多面广多样化情况十分相似，因此PON技术应用于电表信息远程自动采集的优势也同样会非常显著。

考虑到末端智能电表业务比较单一，带宽需求也不是很高，因此选择总线方式利用RS-485线将若干电表串接在一起，信息经初步汇集后再通过PON 进行传送，可实现资源优化配置、建设运营低成本目标。在实际部署时，OLT 通常安装在接入配电室或变电站内，ONU可安装在楼层电表箱或设备间内，光分路器的安装位置可根据OLT 覆盖范围及安装条件灵活选择（如光缆交接箱、光纤接头盒内或ODF 上）。

3. 电力线载波技术

电力线载波技术电力应用如下。

（1）在自动抄表系统中的应用

随着通信技术的不断发展，基于低压配电线的载波抄表系统突显其独有的优势，使得电力行业集中抄表系统稳定在低压电力线载波集中抄表系统（全载波抄表），以及RS-485总线、低压电力线载波混合集中抄表系统（半载波抄表）两种方案上。由于低压电力线载波通信独有的特点（无须额外敷设任何通信电缆、通信组网灵活、地址管理简单、安装施工简单、维护量低等），使其成为集中抄表系统首选的通信方式。

（2）基于互联网+的路灯照明系统

该系统以智能硬件技术与云平台技术为核心，结合电力载波通信技术，实现路灯系统大规模扩展以及网络化控制。使管理人员可以通过PC监控中心及手持设备APP端对系统进行远程监控，从而有效降低路灯系统的建设成本和管理成本。同时，利用云端大数据处理的特点，为路灯照明系统提供信息存储、故障分析、授权管理等增值服务。

电力线载波通信技术及相关产品作为接入网重要的通信方式，可用于配电自动化、用电信息采集、分布式发电与微电网接入等业务；也可扩展应用于“四表集抄”、能效监测、节能管理、智能家居、环境监测等场景的接入侧通信。

4. 卫星通信技术

1）北斗技术电力应用预测

（1）应急通信指挥系统

基于北斗卫星的电力应急通信提高了应急状态下处理突发事件的能力，最大限度地减少其突发事件造成的危害。

（2）统一车辆管理平台

基于定位导航技术可以建设统一车辆管理平台，规范公司用车管理，加强车辆安全管控，提升公司车辆管理精益化水平。

（3）使用输变电线路进行地质灾害监测

基于精准定位服务器，向各省提供输变电线路地质灾害监测服务，提高输变电运行和管理水平，完备灾害应急机制。

利用北斗短报文解决无公网信号地区的电量采集、配网监测、应急故障等问题，提升了各省市公司电网设备管理的精益化程度。

① 调度。安徽省地调控中心建设北斗数据传输终端121台、指挥机2台、管理系统1套。

② 用电信息采集。青海、冀北和四川等八省建设北斗数据终端1965台、指挥机24台、管理系统5套。

③ 应急车辆管理。四川信通公司建设车载终端5台、指挥机1台、管理系统1套。

④ 配网终端监测。冀北运检部建设北斗数据终端70台、指挥机1台、管理系统1套。

授时授频功能主要应用于电网控制领域和管理信息领域，精确一致的时间保障了电网运行的稳定与可靠性，也保障了管理信息的同步性与及时性。

⑤ 电网控制领域。现在已有11类816套调度主站自动化系统接入了北斗授时信号，占比90%；20%的变电站时间同步装置已接收北斗授时信号。新建及改造变电站北斗卫星授时接入率达100%。

⑥ 管理信息领域。管理信息大区中北京、上海、西安三地灾备中心建成以北斗信号为主的一级时间源节点。授时功能在管理信息大区应用实现100%。

2）宽带卫星通信技术电力应用

（1）电力系统通信网络

目前的电力系统通信网络主要由微波（点对点、一点多址、扩频）、光纤通信、电力线载波等地面通信方式组成，已建成了覆盖国家电网、大区电网、省内电网、地区电网的电力系统通信网络。但在地区电网通信网络建设中，总有若干地处偏远的变电所或发供电基层部门，由于电网结线限制或地理环境恶劣、位置偏远，采用地面通信方式或是无法保证传输要求（载波多次转接），或是因需要多次微波中继、架设长距离通信光缆等原因致使方案的性价比很低而无法采用。而卫星通信方式以其通信质量高、建站费用不受通信距离和地理环境限制、覆盖面积辽阔、连接环节少、信道容量大、抗地面灾害、开通快捷、操作维护方便等特点，成为解决这些站点通信需求的最佳选择。

（2）电力应急指挥系统

应急卫星通信是电力应急指挥系统中一个重要的组成部分，在某些特殊情况下（如地震灾害）能发挥无法替代的作用。多数电力应急指挥系统是在现有通信、网络、应用、信息文字、声音、图像、视频的基础上通过应用整合、业务整合、数据整合建立起来的。“5・12”汶川大地震强有力地证明了在地面有线、无线通信基础设施遭到破坏后，卫星通信可以作为很好的应急通信手段。

5. 通信安全技术

1）可信计算技术电力应用

现阶段，我国电网的发展已经进入了“电力流、信息流、业务流”高度融合的智能电网阶段，电网调度控制系统、配电自动化系统以及通信网络成为智能电网的“大脑”与“神经中枢”，管理并控制电网的可靠运行。网络空间的信息安全对电网调度控制系统、配电自动化系统以及通信网络的破坏，对智能电网的实体形成致命的威胁。

电力监控系统经过第一阶段基于边界安全的纵深防护体系及第二阶段基于等级保护的业务安全防护体系的建立，形成了智能电网调度控制系统安全防护的3道防线、层次化的保护体系以及业务级的灾备体系，整体防护能力日益加强。而与此同时，国际信息安全形势不断发展、网络战争形态以及能力的演进，使得大量新型攻击方式快速涌现。“震网”病毒被认为是第一个对工业实体设施形成破坏能力的网络战武器，它突破了控制网络物理

隔离的“封堵”，成功攻击了伊朗核电站。安全威胁特征代码库的迅速增长，使得以“查杀”为核心的被动安全措施对实时控制系统安全防护失去效率。

为应对网络战环境下复杂的信息安全威胁，同时减小防护机制对电力控制系统实时性能的影响，中国正在通过自主创新的可信计算来获得可具有免疫能力的新计算体系结构，通过建立主动防御体系，来弥补网络安全的“老三样”病毒、检测、防护的不足，并已经在电网电力调度领域获得应用。生产控制大区具备控制功能的系统，应用可信计算技术实现计算环境和网络环境安全可信，建立对恶意代码的免疫能力，应对高级别的复杂网络攻击。

面对终端通信接入网涉及云计算、大数据、移动互联网、虚拟动态等新的计算环境，可信计算体系的架构使得在终端通信接入网复杂的网络环境下，实现体系结构可信、操作行为可信、资源配置可信、数据存储可信、策略管理可信的目的。

2）量子通信技术电力应用

① 国网信息通信产业集团有限公司支撑杭州“G20峰会”电力保障

系统针对2016年9月4—5日杭州G20峰会保障需求，在国网浙江电力杭州供电公司应急指挥中心核心机房及G20保电指挥现场部署量子密钥管理系统、量子VPN网关、网络交换机、音视频指挥电话等软硬件，如图8-17所示。利用节点间现有空余纤芯构建量子密钥传输通道，实现杭州G20保电指挥部与G20会场保障指挥部之间的语音、视频及敏感数据的量子保密传输，有效提高G20杭州峰会保电指挥系统信息传输安全。同时，为量子通信技术在电网电视电话会议业务、监控业务中的应用提供技术验证，为后期杭州城域网、“沪杭干线”及浙江省域网建设奠定基础。

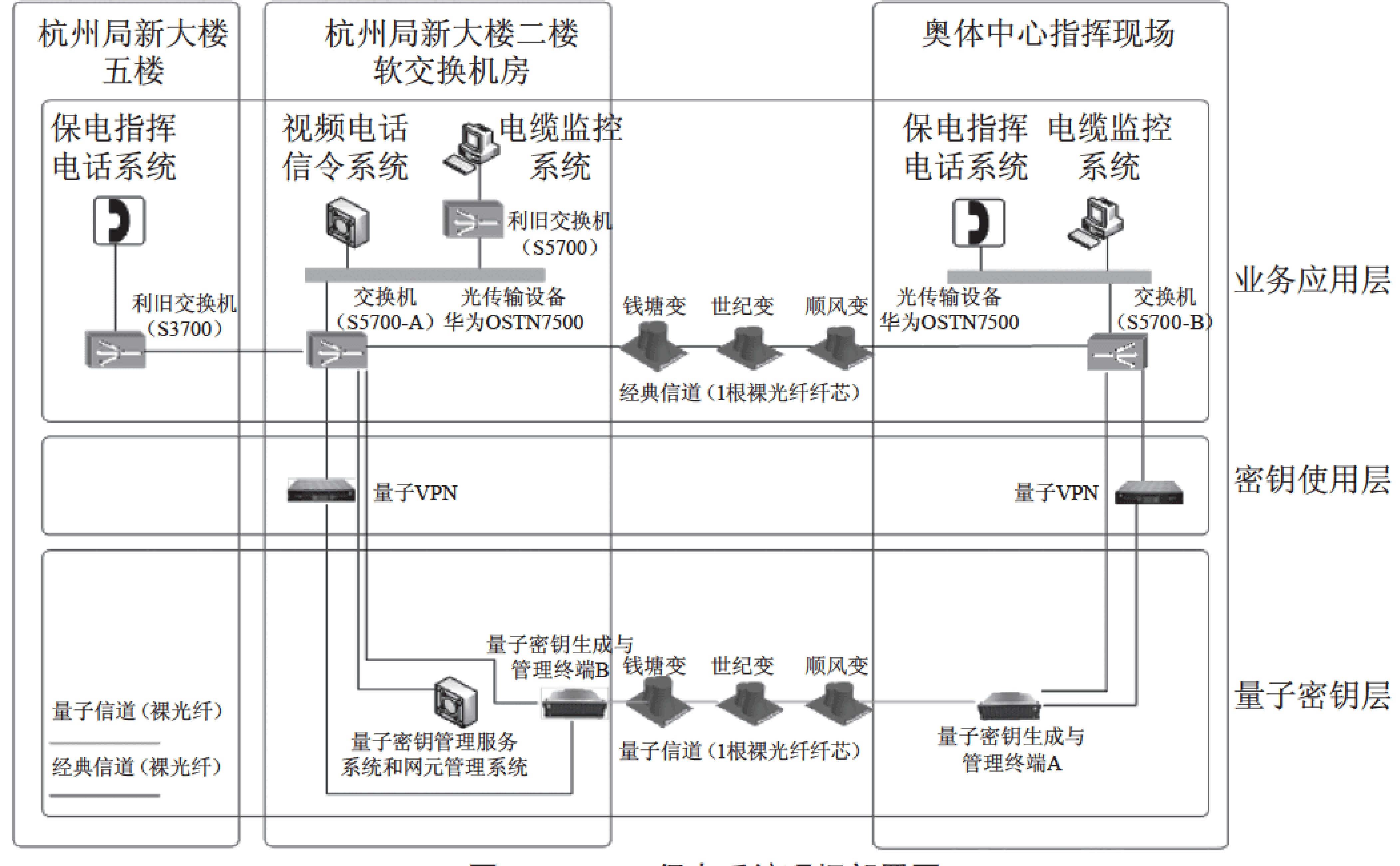


图8-17 G20保电系统现场部署图

② 国网信通产业集团支撑公司两会通信安全保障

国网信通产业集团、科大国盾量子技术股份有限公司基于量子保密通信技术实现公司两会通信安全保障，从管理学院应急通信车至西单二楼应急指挥中心的视频画面通过量子加密通信技术进行安全传输。视频会议系统业务数据从西单通过量子VPN加密后，经过模式口卫星发射中心将信号转发至管理学院，再通过管理学院卫星车接收转发的数据后由量子VPN解密至视频会议系统，如图8-18所示。

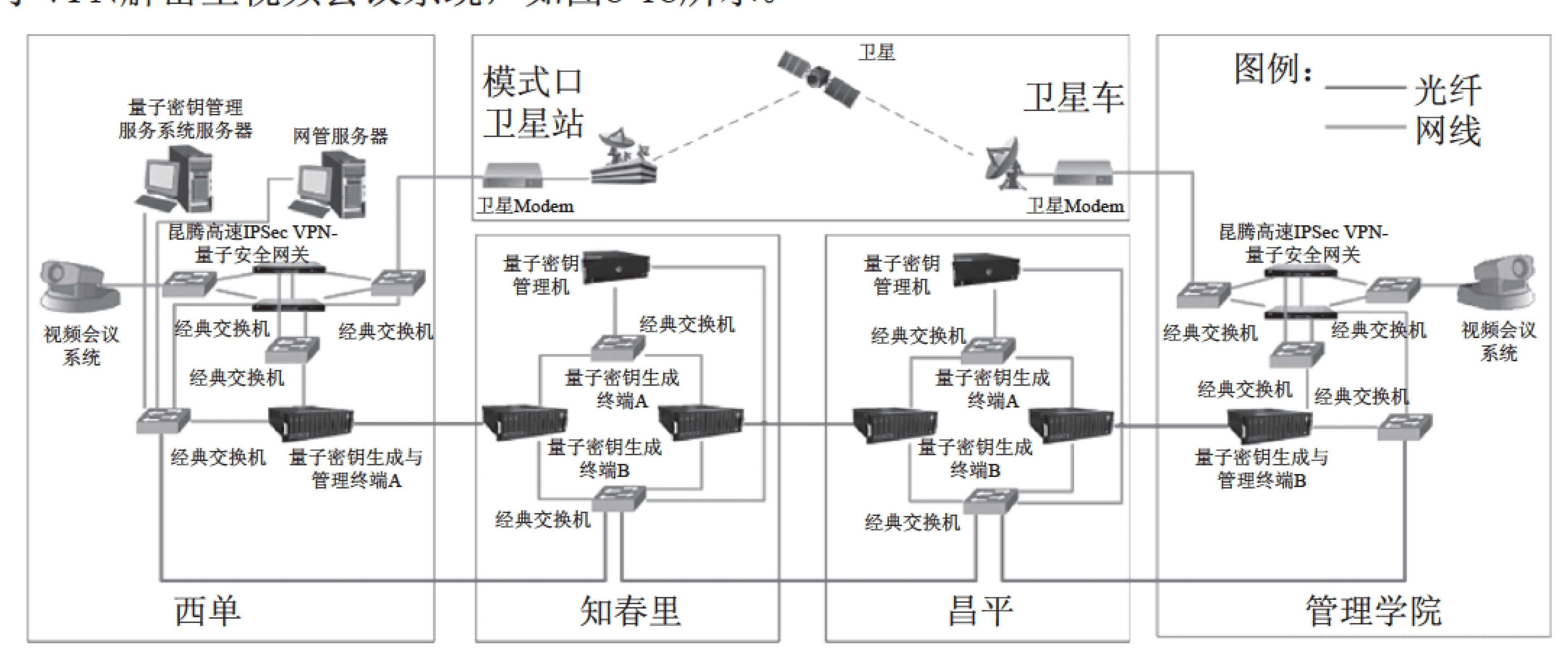


图8-18 两会保障业务量子保密通信系统网络拓扑

③ 安徽电力架空光缆量子保密通信性能测试

2016年，国网安徽省电力公司及科大国盾公司在安徽合肥肥西变电站到肥东众兴变电站开展电力架空光缆量子保密通信性能测试，架空光缆全长68km，路径衰减约15.7dB。测试过程中，两个站点的两台配对工作的QKD设备在长距离悬空光缆信道条件下进行工作，系统组成结构如图8-19所示。项目首次实现量子通信设备在电力架空电缆的环境下天候工作，通过应用快速偏振反馈相关技术，解决了环境频繁扰动所引起的光纤双折射效应对光子偏振态的干扰，同时对两组非正交偏振态进行跟踪、反馈，确保了量子通信在复杂架空光缆的环境下正常成码。

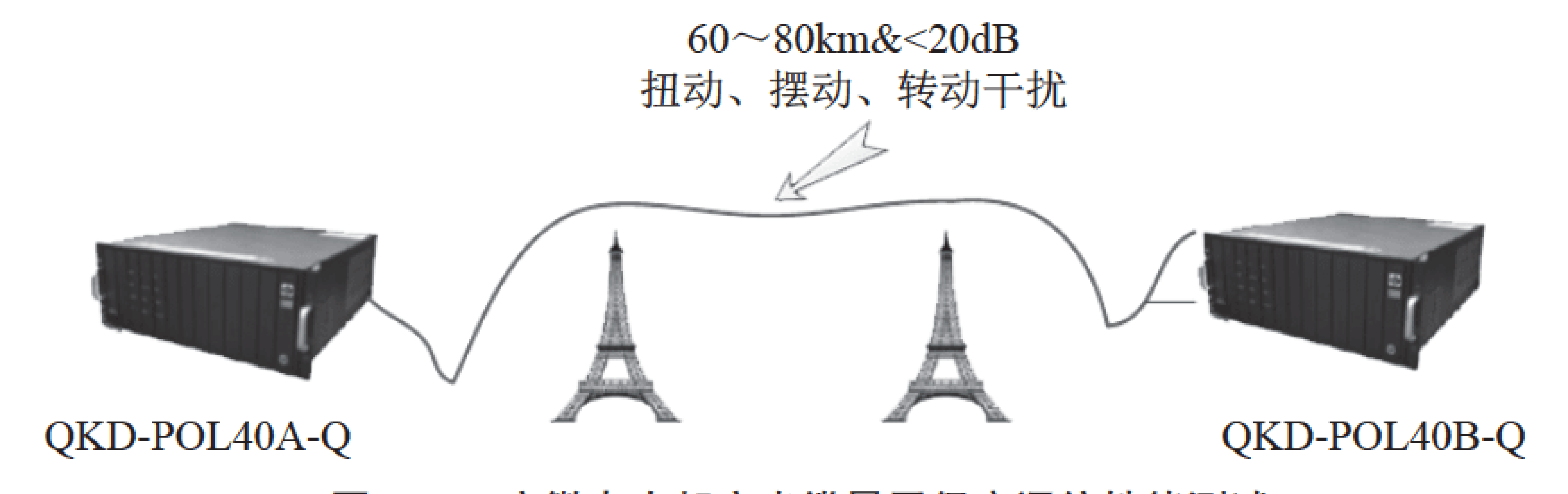


图8-19 安徽电力架空光缆量子保密通信性能测试

④ 电力光缆量子保密通信试验

2012年，国网公司建立了±800kV直流特高压环境、500kV交流特高压环境以及风振舞动环境下的量子密钥分配系统，初步验证OPGW、ADSS和OPPC三种典型电力特种光缆

量子通道传输的可行性。

3）光锁技术电力应用

光通信是网络互联的骨干动脉、网络通信的物理载体和网络空间竞争的重要阵地。作为一种通用关键安全技术，可用于电力光纤网络敷设之处，兼顾了高速通信与信息加密的性能要求，实现了由电接口安全到光接口安全，显著增强了高速信息网络保密通信能力。

4）区块链技术电力应用

能源互联网系统中，交易将呈现多元化、分散化、即时化特征。为使交易更加便捷且低成本，未来能源互联网交易模式趋势之一将是扁平化和“去中心化”。未来发电端随机性增加，同时也会分布化；电网的拓扑结构也会随着电源的分布化和随机化而发生变化；消费者角色将前所未有地在整个能源行业的价值链当中被突出，成为真正的价值链推动者和价值链龙头，通过各种各样的智慧能源方案成为Prosumer，与电源和电网进行良性的有效互动；储能作为电力价值链上的新环节，会成为很重要的缓存和硬盘角色。

2016年上半年，北京全球首个能源区块链实验室建立，能源区块链旨在将大量由分布式能量采集装置，分布式能量储存装置和各种类型负载构成的新型电力网络、石油网络、天然气网络等能源节点互联起来，以电力系统为纽带，利用互联网思维和技术改造能源产业，从而构建横向多元互补、纵向源网荷储协调、能源与信息高度融合的新型能源供用体系。

区块链数据在能源领域主要应用于三个方面：智能电表数据发布及管理、发电厂的尽职调查、点对点能源交换。能源区块链对信息的数据化和网络化使之便于集中传输和处理，提升系统处理能力；能源区块链的公私钥等加密技术能防止虚假交易和记录篡改，便于形成交易主体自律性和系统信用体系；区块链的“去中心化”可有效提升交易效率，降低交易成本；区块链中的主体链（共有链）将各行业价值链进行串联，构建新型能源生态圈。

8.7 总　　结

智能配用电系统是电力企业与电力用户的联系枢纽，终端通信接入网（以下简称“接入网”）作为配用电业务的重要承载网络，涵盖包括配电自动化、用电信息采集、电动汽车充换电站、配变监测、智能台区、分布式能源接入等需求差异较大的业务。构建 “架构合理、性能可靠、安全可控、成本适中”的接入网已成为配用电系统建设的目标。终端通信接入网的规划与建设应结合电网发展和通信技术特点，围绕逐步建设能源互联网的战略目标，积极跟踪通信技术发展，采取跟踪、研究、分析和应用的步骤，科学、合理地选择先进成熟适用的通信技术。

结合全球能源互联网对新能源消纳提出的要求，面对“十三五”期间国家加大投资力度促进配电网规模和智能化水平的不断提升，以及“互联网＋”“大、云、物、移”等新技术应用对电网运行及用户数据采集量的不断增加，向接入网的支撑提出越来越高的要求。本章详细介绍了终端通信接入网建设所用到的新型通信技术，从技术的基本原理、涉及的关键技术以及应用场景对每种新型通信技术进行了全方位的描述，为终端通信接入网的建设提供了技术保证。

参考文献

[1] Smith S W. 可信计算平台：设计与应用[M].北京：清华大学出版社，2006.

[2] 赵明欣，刘伟，陈海，等. 《配电网规划设计技术导则》解读[J]. 供用电，2016(2)：2-7.

[3] 齐一飞，金学东，刘振栋，等. 烟台地区“十三五”配电通信网规划研究[J]. 电力信息与通信技术，2015，13(7)：65-68.

[4] 刘海波，胡滨，王旭阳. 关于“十三五”配电网发展的思考[J]. 中国电力，2015 (1)：21-24.

[5] 杨震中. 接入网光纤化的部署[J]. 光纤通信技术，1996 (6)：9-15.

[6] 王立鹏，任顺航，吕鹏鹏，等. 基于用电信息采集系统的通信技术[J]. 电子科技，2013，26(11)：170-172.

[7] 佚名. 配电自动化建设与改造标准化设计技术规定[C]. 配电自动化新技术及其应用高峰论坛. 2011.

[8] 曹津平，刘建明，李祥珍. 面向智能配用电网络的电力无线专网技术方案[J]. 电力系统自动化，2013，37(11)：76-80.

[9] 严辉，李庚银，赵磊，等. 电动汽车充电站监控系统的设计与实现[J]. 电网技术，2009，33(12)：15-19.

[10] 赖振学. 智能电网技术[M]. 北京：中国电力出版社，2013.